Authenticator with sequential memory storage

Patent number: FR2592502
Publication date: 1987-07-03
Inventor:
Applicant: LEFEVRE JEAN PIERRE (FR)
Classification:
- international: G06K7/01; G06K19/00; G06F13/10; G06F12/14
- european: G07C9/00B6B; G07F7/10C4; G06K7/00K2; G07F7/10D4E; G07F7/10D8P
Application number: FR19850019257 19851226
Priority number(s): FR19850019257 19851226

Abstract of **FR2592502**

The invention relates to an apparatus and its associated operating method for checking the identity of a user for the purposes of authorising access to protected resources or to the use of reserved services. The authenticator with sequential memory storage whose operation is stand-alone or associated with that of the software of a computer system executes an information authentication algorithm which can take account of:

- a secret personal code,
- a random code delivered by the specialised software of a computer system,
- a public or secret encryption key,
- the secret code recorded in a microprocessor card, read by an optional device incorporated in the authenticator,
- the last code generated by the apparatus.

The authenticator with sequential memory storage is portable but it may also be incorporated into another item of equipment.

---

(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 592 502**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **85 19257**

(51) Int Cl⁴ : G 06 K 7/01, 19/00; G 06 F 13/10 // G 06 F 12/14.

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 26 décembre 1985.

(30) **Priorité :**

(43) **Date de la mise à disposition du public de la demande :** BOPI « Brevets » n° 27 du 3 juillet 1987.

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *LEFEVRE Jean Pierre.* — FR.

(72) **Inventeur(s) :** Jean Pierre Lefèvre.

(73) **Titulaire(s) :**

(74) **Mandataire(s) :**

(54) Certificateur à mémorisation séquentielle.

(57) L'invention concerne un appareil et son procédé de fonctionnement associé afin de contrôler l'identité d'un usager dans le but de l'autoriser à accéder à des ressources protégées ou à utiliser des services réservés.

Le certificateur à mémorisation séquentielle dont le fonctionnement est autonome ou associé à celui du logiciel d'un système informatisé exécute un algorithme de certification d'informations qui peut prendre en compte :

— un code secret personnel,

— un code aléatoire délivré par le logiciel spécialisé d'un système informatisé,

— une clef publique ou secrète de chiffrement,

— le code secret enregistré dans une carte à microprocesseur, lu par un dispositif optionnel incorporé au certificateur,

— le dernier code généré par l'appareil.

Le certificateur à mémorisation séquentielle est portatif mais il peut également être incorporé dans un autre matériel.

FR 2 592 502 - A1

Vente des fascicules à l'IMPRIMERIE NATIONALE, 27, rue de la Convention — 75732 PARIS CEDEX 15

La présente invention concerne un certificateur à mémorisation séquentielle et le procédé pour faire fonctionner les dispositifs de l'appareil dans l'objectif de :

- identifier et authentifier avec certitude une personne physique afin de l'autoriser à se connecter à un système informatisé,
- effectuer un contrôle permettant d'affirmer qu'aucun accès illicite au sein du système informatisé n'a été effectué par des tiers,
- apporter la preuve irréfutable des connexions successives de la part d'un usager autorisé, au système informatisé,
- assurer l'identification et/ou l'authentification entre deux interlocuteurs géographiquement distants,
- générer une signature informatique attestant de l'identité et de la volonté du donneur d'ordre, de la chronologie des actions, de la conformité et de l'intégrité de l'instruction ordonnée et des informations transmises,
- identifier et authentifier avec certitude une personne physique afin de l'autoriser à accomplir certaines actions pour lesquelles elle a reçu délégation,
- compléter éventuellement la procédure habituelle d'identification de l'usager, par l'utilisation d'une carte à microprocesseur,
- chiffrer une information, par exemple un code secret personnel, pour le transmettre à un tiers ou à un système informatisé.

Ces différents objectifs sont basés sur le contrôle ultérieur par :

- le logiciel spécialisé d'un système informatisé,
- un autre certificateur à mémorisation séquentielle.

Ce contrôle repose sur l'exécution par le certificateur d'un algorithme de certification et/ou de chiffrement.

En fonction des options choisies par l'utilisateur, l'algorithme met en oeuvre :

- un code secret personnel et/ou une carte à microprocesseur,
- un code aléatoire, délivré par le logiciel spécialisé d'un système informatisé,
- une clef publique de chiffrement,
- une clef secrète de chiffrement.

Le domaine technique auquel se rapporte l'invention est

celui du contrôle de l'identité d'une personne physique dans le but de l'autoriser à :

- accéder à des ressources protégées, par exemple : un fichier ou une transaction informatique en relation avec des informations confidentielles,
- utiliser un objet ou un service, par exemple : une carte de crédit, un chèque bancaire, etc ...
- contribuer à l'élaboration d'un document "sensible", par exemple l'ordonnancement d'un dossier financier, en apportant la preuve formelle de l'identité de l'émetteur, tout en lui interdisant la possibilité de renier ultérieurement cette action, par la mise en oeuvre du concept de la signature informatique,
- se faire reconnaître d'un tiers accrédité dans le cadre de l'échange d'informations précieuses ou confidentielles.

Le contrôle de l'identité d'une personne physique, communément nommé "authentification" est généralement basé sur la reconnaissance d'un code secret numérique ou alphanumérique. Ce code secret est la propriété de chaque individu.

La procédure d'authentification d'une personne physique est en général la suivante :

- l'utilisateur communique au système informatisé son identité en composant sur le clavier d'un terminal, un code d'identification,
- le système informatisé, afin d'effectuer le contrôle de la validité de ce code d'identification demande à la personne concernée de fournir une information particulière permettant au système de s'assurer qu'il n'y a pas eu usurpation d'identité,
- cette information est habituellement transmise au système informatisé par l'usager sous la forme d'un code secret. Le logiciel spécialisé du système informatisé compare le code secret communiqué, avec le code secret de référence, conservé dans une mémoire particulière ou dans un fichier protégé. Si les deux codes sont identiques, la personne est autorisée à accéder aux ressources du système informatisé, sinon l'autorisation est rejetée.

Cette procédure présente les inconvénients suivants :

- risque de divulgation des codes secrets car l'usager doit

prendre de réelles dispositions afin de conserver le caractère confidentiel de son code secret personnel (notamment, lorsqu'il le compose sur le clavier du terminal permettant l'accès au système informatisé),

- risque de divulgation du code secret personnel lors de l'acheminement par le réseau de transmission de données au système informatisé,
- obligation pour l'utilisateur de procéder régulièrement au changement de son code secret personnel en raison des risques de divulgation énoncés précédemment. Cette procédure de changement est très contraignante pour l'utilisateur et de ce fait, peu observée dans la pratique, augmentant ainsi la vulnérabilité des systèmes informatisés, et les chances de réussir des accès illicites,
- complications supplémentaires dans l'exécution du travail de l'utilisateur, en raison de ses besoins éventuels d'accéder à des systèmes informatisés différents qui le contraigne à connaître, retenir et gérer de multiples codes secrets.

A l'inverse, la criminalité informatique par connexions illicites ou frauduleuses aux systèmes informatisés tend à généraliser l'obligation d'authentifier avec certitude les personnes qui demandent à se connecter. Cette obligation est encore renforcée lorsqu'il s'agit d'exécuter certaines transactions, l'accès à des programmes informatiques sensibles, à des données élémentaires confidentielles, à des ressources critiques du système d'exploitation de l'ordinateur.

Pour d'autres cas, le contrôle de l'identité d'une personne physique utilisant un objet ou un service, par exemple une carte de crédit, un chèque bancaire est généralement basé sur l'examen visuel d'une pièce d'identité, d'une signature manuscrite, des informations d'un laissez-passer, etc ...

Malheureusement ces contrôles peuvent se révéler inefficaces en raison de l'ingéniosité de certain falsificateur, fraudeur ou voleur. C'est le cas par exemple pour les cartes de crédit ou les carnets de chèques, pour lesquels il est pratiquement impossible de s'assurer que ceux ci sont bien la propriété de la personne qui tente d'en

faire usage.

La présente invention qui a pour objectif d'apporter une solution aux problèmes évoqués sera mieux comprise à la lecture de la description du certificateur à mémorisation séquentielle, complétée des procédés de fonctionnement pour les utilisations correspondantes, dans le cadre de :

- l'authentification de l'identité d'une personne physique,
- la modification des données enregistrées dans le module de mémoire du certificateur,
- la certification d'une information à l'aide du procédé de la signature informatique,
- la génération d'un code de certification chronologique,
- la génération d'une signature informatique,
- le chiffrement d'une information, par exemple : un code secret personnel.

Un complément d'information est apporté par les figures suivantes :

- la figure 1 est une vue en perspective du certificateur à mémorisation séquentielle,
- la figure 2 est un schéma représentant la procédure adoptée, combinant les actions exécutées par l'utilisateur à l'aide du certificateur et par le système informatisé et qui décrit l'enchaînement obligatoire des actions nécessaires pour effectuer une opération d'authentification d'identité, ayant pour principe l'échange d'un code aléatoire,
- la figure 3 est un ordinogramme représentant la logique du principe adopté pour l'enchaînement des actions de l'utilisateur, effectuées à l'aide du certificateur, au cours d'une opération d'authentification d'identité d'une personne physique,
- la figure 4 est un ordinogramme représentant la logique du raisonnement adoptée dans l'algorithme de certification, enregistré dans le module de mémoire du certificateur et dans le logiciel spécialisé du système informatisé,
- la figure 5 est un tableau représentant un exemple de la configuration de trente sept des deux cent cinquante six postes de quatre nombres de deux chiffres utilisée par l'algorithme de certification, enregistrée dans le module de mémoire du certificateur et dans le logiciel spécialisé

du système informatisé,

- la figure 6 est un tableau représentant un exemple de la configuration de trente sept des deux cent cinquante six postes de quatre nombres de trois chiffres utilisée par l'algorithme de certification, enregistrée dans le module de mémoire du certificateur afin de générer une signature informatique,

- la figure 7 est un ordinogramme représentant la logique du principe adoptée pour l'enchaînement des actions de l'utilisateur effectuées à l'aide du certificateur, lors des opérations de modification pour le module de mémoire :
  . du code secret,
  . du code standard de certification,
  . de la clef secrète de chiffrement,
  . des quatre zones réservées pour les dialogues avec la carte à microprocesseur,
  . et pour chacune des trente et une entrées de la table :
    - l'identité de l'utilisateur et le type de traitement employé,
    - le(s) code(s) secret personnel,
    - la clef publique de chiffrement,
    - la clef secrète de chiffrement,
    - le dernier code de certification généré,
    - l'avant dernier code de certification généré,
    - la dernière signature informatique générée,
    - l'avant dernière signature informatique générée,
  . des deux cent cinquante six postes de la table de certification,

- la figure 8 est un ordinogramme représentant la logique du principe adopté pour l'enchaînement des actions du responsable habilité qui sont effectuées à l'aide du certificateur à mémorisation séquentielle, au cours d'une opération de certification d'informations sensibles afin d'authentifier un ordre donné, par la génération d'une signature informatique ou d'un code de certification,

- la figure 9 est un ordinogramme représentant la logique du principe adopté pour l'enchaînement des actions du responsable habilité et de l'utilisateur, qui sont effectuées à l'aide du certificateur à mémorisation séquentielle, au cours d'une opération manuelle d'authen-

tification d'identité, par la génération de signature informatique,

- la figure 10 est un schéma représentant la procédure adoptée, combinant les actions exécutées par l'utilisateur à l'aide du certificateur à mémorisation séquentielle et par le système informatisé et, qui décrit l'enchaînement obligatoire des actions nécessaires pour effectuer une opération d'authentification d'identité, reposant sur la génération, l'échange et la mémorisation séquentielle de code de certification,
- la figure 11 est un schéma fonctionnel représentant l'organisation interne du module de mémoire du certificateur,
- la figure 12 est un schéma fonctionnel représentant les échanges d'informations et le sens de ces échanges au niveau des principaux composants électroniques du certificateur à mémorisation séquentielle. C'est également un schéma-bloc illustrant les caractéristiques fondamentales du montage électrique,
- la figure 13 est un plan (vue de dessus) du mécanisme assurant la lecture de la carte à microprocesseur, installé dans le certificateur à mémorisation séquentielle,
- la figure 14 est un plan (vue en coupe) du mécanisme assurant la lecture de la carte à microprocesseur, installé dans le certificateur à mémorisation séquentielle. Sur ce plan, la carte à microprocesseur n'est pas introduite dans le mécanisme,
- la figure 15 est un plan (vue en coupe) du mécanisme assurant la lecture de la carte à microprocesseur, installé dans le certificateur à mémorisation séquentielle. Sur ce plan, la carte à microprocesseur est introduite dans le mécanisme de lecture.

Le certificateur à mémorisation séquentielle représenté sur la figure 1 comporte un carter constitué par un couvercle (1) et un fond reliés ensemble de manière appropriée, par exemple par des vis. Le carter comprend une fente (13) qui permet d'introduire une carte à microprocesseur (14) de format standard dans le mécanisme de lecture, représenté sur les figures 13, 14, et 15, qui équipe en option le certificateur à mémorisation séquentielle.

Le couvercle (1) comporte une ouverture (15) derrière laquelle est placée un écran standard d'affichage (2) permettant à l'utilisateur de visualiser des informations ou instructions. Le couvercle (1) comporte également l'ouverture (17) à travers laquelle fait saillie l'interrupteur (16) de mise en fonction et hors fonction du certificateur. Le couvercle (1) comporte également les ouvertures (18), (19), (20), (21), (22), (23), (24) à travers lesquelles font saillies respectivement les touches de fonction : IDENTIFIER (5), AUTHENTIFIER (6), CERTIFIER (7), SIGNER (8), INITIER (9), ENTRER (10), EFFACER (11). Le couvercle (1) comporte également les ouvertures (25), (26), (27), (28), (29), (30), (31), (32), (33), (34), (35), (36), (37), (38), (39), (40), (41), (42), (43), (44), (45), (46), (47), (48), (49), (50), (51), (52), (53), (54), (55), (56), (57), (58), (59), (60) à travers lesquelles font saillies respectivement les touches alphabétiques : A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y, Z, numériques : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, et les touches de défilement gauche : ← et droite : → référencées par la suite clavier alphanumérique (12).

Le mécanisme de lecture de carte à microprocesseur accessible par l'intermédiaire de la fente (13), représenté sur la figure 13, est composé des éléments suivants :

- une carte (237) à microprocesseur (242) conforme à la norme standard,
- une fente (238) permettant d'introduire manuellement la carte à microprocesseur, laquelle viendra se placer contre la plaquette (239 maintenue sur le support (251) du mécanisme de lecture par les vis (245), (246), (247), et (248),
- quatre barrettes métalliques (240) permettant d'assurer les contacts avec les plots de gauche du microprocesseur (242), maintenues par une languette non conductrice (243) fixée sur la plaquette (239) par deux vis et reliées aux composants électroniques du lecteur par quatre fils de connexion (250),
- quatre barrettes métalliques (241) permettant d'assurer les contacts avec les plots de droite du microprocesseur (242), maintenues par une languette non conductrice (244) fixée sur la plaquette (239) par deux vis et reliées aux compo-

sants électroniques du lecteur par une seconde série de quatre fils de connexion (250),

- un contacteur (249) chargé de détecter la présence de la carte à microprocesseur dans le lecteur et dans l'affirmative, de déclencher l'alimentation électrique pour le microprocesseur (242).

Les vues en coupe représentées sur les figures 14 et 15 permettent de mieux comprendre le principe de fonctionnement du lecteur de carte à microprocesseur.

La figure 14 représente le mécanisme de lecture au repos :

- les biseaux de la fente (252) permettent de faciliter l'introduction de la carte à microprocesseur (237),
- la plaquette (239) est maintenue contre le support (251) du mécanisme de lecture par l'intermédiaire des vis (257) (258) et des ressorts (259), (260) correspondantes aux vis (245) et (246) de la figure 13. Les vis (247) et (248) n'étant pas représentées sur la figure 14.
  L'ensemble est maintenu solidaire avec le boitier (262) du certificateur par la(les) vis (261),
- les barrettes métalliques (253) et (254) sont maintenues contre la plaquette (239) par les vis (255) et (256).

La figure 15 représente le mécanisme lorsqu'une carte à microprocesseur (237) a été introduite manuellement par l'utilisateur :

- la plaquette (239) est maintenue contre la carte à microprocesseur (237) par les ressorts (270) et (271) fixés par les vis (268) et (269) correspondantes aux vis (245) et (246) de la figure 13. Les vis (247) et (248) n'étant pas représentées sur la figure 15.
- les barrettes métalliques (264) et (265) fixées par les vis (266) et (267) s'écartent légèrement de la plaquette (239) mais gardent le contact avec les différents plots du microprocesseur (242).
  L'ensemble est maintenu solidaire avec le boitier (273) du certificateur par la(les) vis (272),
- lorsque l'utilisateur procède au retrait de la carte à microprocesseur (237) les barrettes métalliques reprennent la position d'origine (253) et (254) de la figure 14.

Dans le carter du certificateur à mémorisation séquentielle représenté sur la figure 1 sont incorporés des composants

mécaniques et électroniques standards d'un point de vue industriel et notamment :

- un écran d'affichage (2) permettant à l'usager de visualiser des informations ou instructions,
- un microprocesseur (3) chargé de gérer les fonctions de base du certificateur et d'exécuter le traitement des algorithmes de certification et/ou de chiffrement,
- un module de mémoire (4) dans lequel sont enregistrés :
  - . le code interne du module. Ce code, constitué de seize octets est accessible pour lecture par le microprocesseur du certificateur. Ce code enregistré lors de la fabrication ne peut pas être modifié par l'utilisateur,
  - . le code secret du module. Ce code, composé de seize octets est accessible par le microprocesseur du certificateur. Ce code, initié lors de la fabrication peut être modifié mais ne peut pas être lu par l'utilisateur,
  - . le code standard de certification. Ce code, constitué de seize octets est accessible par le microprocesseur du certificateur. Ce code, initié lors de la fabrication peut être modifié mais ne peut pas être lu par l'utilisateur,
  - . la clef secrète de chiffrement. Cette clef composée de seize octets doit être initiée par le responsable habilité, avant la première utilisation du certificateur. Cette zone ne peut pas être lue par l'utilisateur,
  - . les quatre zones réservées pour les dialogues avec la carte à microprocesseur,
  - . une table à trente et une entrées, chacune desquelles étant composées de quatre zones de seize octets dans lesquelles sont enregistrées :
    - l'identité de l'utilisateur et le type de traitement décidé,
    - le(s) code(s) secret personnel,
    - la clef publique de chiffrement,
    - la clef secrète de chiffrement,
    - le dernier code de certification généré,
    - l'avant dernier code de certification généré,
    - la dernière signature informatique générée,

- l'avant dernière signature informatique générée,

cette table, vierge lors de la fabrication du certificateur est initiée progressivement par le(s) utilisateur(s),

. une table à deux cent cinquante six entrées de seize octets dans lesquelles sont enregistrées les valeurs correspondantes au code de certification retenu. Cette table initiée lors de la fabrication peut être modifiée par l'utilisateur,

. une zone de huit mille cent quatre vingt douze octets dans laquelle est enregistrée le programme exécuté par le microprocesseur du certificateur.

En règle générale, l'initiation des différentes zones ou tables ne peut être réalisée que par un utilisateur habilité, c'est-à-dire disposant :

- du code interne du module de mémoire,
- du code secret du module de mémoire,

implantés dans le certificateur à mémorisation séquentielle.

Pour des besoins spécialisés, le module de mémoire peut être inhiber et remplacer par un module de mémoire externe enfichable, présentant les mêmes caractéristiques fonctionnelles.

Le certificateur à mémorisation séquentielle et le procédé pour faire fonctionner les dispositifs de l'appareil en liaison étroite avec le logiciel spécialisé d'un système informatisé, est caractérisé par le principe de base décomposé sur la figure 2 et dont la description est donnée ci après.

Lorsqu'un utilisateur exécute une procédure standard de connexion à un système informatisé (61), le logiciel spécialisé de ce système reçoit le message composé par l'utilisateur sur le clavier de son terminal, dans lequel est inclu le code d'identification nécessaire, par exemple : DUPONT.

Le logiciel spécialisé du système informatisé mémorise ce code d'identification et adresse en retour (62) à l'utilisateur, un message alphanumérique fabriqué par un algorithme spécifique, par exemple : ZDBXEC4F. Ce message est affiché par le système sur l'écran de visualisation du terminal de l'utilisateur.

A l'aide du certificateur à mémorisation séquentielle, l'utilisateur réalise (63) les étapes représentées sur la figure 3 :

- mise sous tension manuelle (66) du certificateur en basculant l'interrupteur (16) sur la position : EN FONCTION,
- le message : IDENTIFIER s'affiche (67) sur l'écran (2),
- l'utilisateur appuie (68) sur la touche de fonction : IDENTIFIER (5),
- un message constitué de tirets est affiché (69) sur l'écran (2),
- l'utilisateur compose (70) le code d'identification, par exemple : DUPONT à l'aide du clavier alphanumérique (12),
- l'utilisateur appuie (71) sur la touche de fonction : ENTRER (10),
- le message : AUTHENTIFIER s'affiche (72) sur l'écran (2),
- l'utilisateur appuie (73) sur la touche de fonction : AUTHENTIFIER (6),
- un message constitué de tirets est affiché (74) sur l'écran (2),
- l'utilisateur compose (75) son code secret personnel, par exemple : CASIMODO, puis appuie (76) sur la touche de fonction : ENTRER (10),
- le message : CERTIFIER s'affiche (77) sur l'écran (2),
- l'utilisateur appuie (78) sur la touche de fonction : CERTIFIER (7),
- un message constitué de tirets est affiché (79) sur l'écran (2),
- l'utilisateur compose (80) le message que lui a délivré l'ordinateur et qui se trouve affiché sur l'écran de visualisation de son terminal, soit dans l'exemple : ZDBXEC4F à l'aide du clavier alphanumérique (12),
- l'utilisateur appuie (81) sur la touche de fonction : ENTRER (10),
- le certificateur exploite (82) par l'exécution de l'algorithme de certification les informations :
  . code d'identification : DUPONT
  . code secret personnel de l'utilisateur : CASIMODO
  . message délivré par l'ordinateur : ZDBXEC4F

. table individuelle de certification,

Cette action est représentée par le repère (63) de la figure 2.

- le résultat du traitement de l'algorithme de certification est affiché (83) sur l'écran (2) du certificateur, sous la forme d'une valeur de huit positions numériques, par exemple : 28121456
- l'utilisateur compose sur le clavier de son terminal connecté au système informatisé, le code de certification élaboré par le certificateur à mémorisation séquentielle, dans notre exemple : 28121456
le terminal le transmet au système informatisé (64) de la figure 2.

Le logiciel spécialisé du système informatisé dispose du même algorithme de certification et des informations :

. code d'identification : DUPONT
. code secret de l'utilisateur : CASIMODO
. message délivré par l'ordinateur : ZDBXEC4F
. table individuelle de certification,

Le logiciel spécialisé exécute à son tour l'algorithme de certification dont le résultat du traitement donne également une valeur de huit positions numériques, soit dans notre exemple : 28121456

Le logiciel spécialisé du système informatisé effectue la comparaison entre le code transmis par l'utilisateur et le code élaboré au cours de l'exécution de l'algorithme de certification. Si les deux codes sont identiques, l'ordinateur authentifie l'utilisateur. Dans le cas contraire, l'ordinateur refuse l'accès de l'utilisateur et prend les dispositions qui s'imposent afin de procéder à son rejet du système informatisé.

Cette action est représentée par le repère (65) de la figure 2.

- pour terminer, l'utilisateur procède manuellement (84) à la mise hors tension du certificateur à mémorisation séquentielle à l'aide de l'interrupteur (16). En cas d'omission, cette mise hors tension sera réalisée automatiquement après un délai de trois minutes, par le microprocesseur du certificateur.

Le certificateur à mémorisation séquentielle et le procédé

pour faire fonctionner cet appareil en liaison étroite avec un logiciel spécialisé d'un système informatisé supprime les inconvénients :

- de divulgation du code secret personnel lors de l'introduction au clavier du terminal ou durant l'acheminement par le réseau de transmission de données, au système informatisé,
- de changement régulier du code secret personnel de l'utilisateur,
- de la nécessité de disposer d'un code secret personnel particulier pour chaque système informatisé qui est accédé par l'utilisateur.

En effet, en raison du raisonnement utilisé dans l'algorithme de certification, dont la description est fournie par la suite, le certificateur à mémorisation séquentielle et l'utilisation de cet appareil conduit à ce que le code secret généré et acheminé (64) au système informatisé est différent quel que soit l'espace de temps écoulé ou les caractéristiques du système informatisé auquel l'utilisateur souhaite accéder. De plus, il ne suffit pas de disposer du certificateur à mémorisation séquentielle pour que le code numérique généré par l'appareil permette à un utilisateur illicite d'être authentifier par un système informatisé puisque le code généré prend en compte le code secret personnel de l'utilisateur, lors du traitement par l'algorithme de certification. Ce code secret, enregistré à la demande de l'utilisateur est chiffré dans le certificateur à mémorisation séquentielle, par conséquent seul l'utilisateur habilité obtiendra son authentification par le logiciel spécialisé du système informatisé. Par ailleurs, une disposition simple, qui ne peut être observée par des tiers, lorsque l'utilisateur procède aux manipulations usuelles sur le certificateur, permet d'alerter le système informatisé que l'utilisateur fait l'objet de contraintes de la part d'individus malveillants. Cette disposition est mise en oeuvre par le logiciel spécialisé du système informatisé.

L'algorithme de certification enregistré dans le module de mémoire du certificateur est également incorporé dans le logiciel spécialisé du système informatisé (65). L'algorithme de certification est caractérisé par un procédé,

dont le raisonnement décomposé sur la figure 4 est décrit à titre d'exemple, ci après :

- l'utilisateur introduit le code d'identification (bloc 85) dont la longueur peut varier entre un et huit caractères alphanumériques,
- le code d'identification est déplacé (bloc 86) pour être enregistré dans la mémoire 106,
- l'utilisateur introduit son code secret personnel (bloc 87) dont la longueur peut varier entre un et huit caractères alphanumériques,
- le code secret personnel est déplacé (bloc 88) pour être enregistré dans la mémoire 107,
- l'utilisateur introduit le code aléatoire (bloc 89) de huit caractères alphanumériques que lui a délivré (62) figure 2, le système informatisé,
- le code aléatoire est déplacé (bloc 90) pour être enregistré dans la mémoire 108,
- la mémoire 109 est initié (bloc 91) à la valeur numérique UN,
- un test (bloc 92) de la valeur numérique enregistré dans la mémoire 109 est effectué afin de déterminer si cette valeur est égale à la valeur numérique VINGT CINQ. Dans l'affirmative, le contrôle du programme est transféré afin de poursuivre l'exécution à l'étape 102,
- les mémoires 106, 107, 108 étant adjacentes forment une mémoire unique de vingt quatre caractères. Une opération de recherche (bloc 93) dans les postes de la table de certification est effectuée afin d'enregistrer (bloc 94) dans la mémoire 111, la valeur numérique correspondante au premier caractère de gauche de la mémoire 106, en raison du fait que la mémoire 109 contient la valeur numérique UN. Puisque le premier caractère est le caractère D (de DUPONT), la valeur numérique qui sera enregistré (bloc 94) dans la mémoire 111 est selon le tableau indiqué sur la figure 5, la valeur numérique : 36534153
- un test (bloc 95) de la valeur numérique enregistré dans la mémoire 109 est effectué afin de déterminer si cette valeur est égale à la valeur numérique UN. Dans l'affirmative, le contrôle du programme est transféré afin de poursuivre l'exécution à l'étape 100, dans laquelle le

contenu de la mémoire 111 est déplacé afin de l'enregister dans la mémoire 113. Un branchement inconditionnel transfert l'exécution du programme à l'étape 98, dans laquelle la valeur numérique UN est additionnée au contenu de la mémoire 109. Un branchement inconditionnel (bloc 99) est opéré afin de poursuivre l'exécution à l'étape 92. Un test de la valeur numérique contenu dans la mémoire 109 est effectué (bloc 92) afin de déterminer si cette valeur est égale à la valeur numérique VINGT CINQ. Dans la négative, le contrôle du programme est transféré à l'étape 93, dans laquelle la valeur numérique correspondante au caractère suivant est recherché afin d'être enregistré (bloc 94) dans la mémoire 111,

- le produit de la matrice enregistrée dans la mémoire 111 par la matrice enregistrée dans la mémoire 113 est calculé en comptant modulo : quatre vingt dix sept, et le résultat est enregistré (bloc 96) dans la mémoire 112,
- le contenu de la mémoire 112 est déplacé pour être enregistré (bloc 97) dans la mémoire 113,
- la valeur numérique : UN est additionnée (bloc 98) à la valeur numérique enregistrée dans la mémoire 109,
- un branchement inconditionnel (bloc 99) est opéré afin de poursuivre l'exécution à l'étape 92,
- lorsque la mémoire 109 contient la valeur numérique VINGT CINQ, la boucle de traitement a été exécutée VINGT QUATRE fois et par conséquent l'ensemble des caractères alphanumériques enregistrés dans les mémoires 106, 107, 108 ont été traduits en valeurs numériques, puis les produits successifs des matrices correspondantes ont été calculés. Le résultat final, c'est-à-dire la clef de certification se trouve enregistrée dans la mémoire 113, dans notre exemple la valeur numérique : 28121456 est affichée (bloc 102) sur l'écran (2),
- une opération de comptage de temps (bloc 103) et de test dans le but de vérifier que le seuil de trois minutes n'a pas été atteint est réalisée. Dans l'affirmative, le contrôle du programme est transféré afin de poursuivre l'exécution à l'étape 105, dans laquelle le microprocesseur (3) effectue la mise hors tension automatique du certificateur. Dans le cas contraire, un branchement

inconditionnel (bloc 104) est opéré afin de poursuivre l'exécution à l'étape 103.

Le procédé de certification mis en oeuvre par l'algorithme exécuté par le certificateur donne la probabilité d'UNE chance sur CENT MILLIONS de découvrir par hasard la valeur exacte que le système informatisé s'attend à recevoir pour authentifier l'identité de la personne qui procède à une tentative de connexion. Etant donné que le système informatisé n'accepte qu'une seule réponse, il apparaît comme peu réaliste d'imaginer que la connexion illicite d'un intru puisse survenir dans ces conditions. Le procédé de certification donne une probabilité de 1/87.000.000 pour que deux combinaisons alphanumériques différentes de VINGT QUATRE caractères donnent une valeur identique.

En résumé, le procédé retenu dans le certificateur est basé sur la création d'une signature informatique, ayant pour origine un ensemble de caractères alphanumériques, désigné par le terme de clef temporaire. La clef temporaire est constituée des informations suivantes :

- code d'identification de l'utilisateur,
- code secret personnel de l'utilisateur,
- code aléatoire, délivré par le logiciel spécialisé d'un système informatisé.

La signature informatique est créée au cours de l'exécution de l'algorithme de certification. La certification associe à chaque caractère (lettre, chiffre) une matrice de rang deux, c'est-à-dire composée d'un tableau carré de quatre nombres. Pour créer la signature informatique, le programme enregistré dans le module de mémoire du certificateur effectue en chaîne les produits des matrices de tous les caractères de la clef temporaire. Afin d'éliminer les risques de dépassement, les calculs sont opérés en modulo : QUTRE VINGT DIX SEPT, soit le plus grand nombre premier de deux chiffres. L'authentification d'identité est considérée acqise si une autre clef temporaire obtenue à partir d'une source différente d'informations, traitée par le même algorithme de certification, dans un équipement informatisé différent, engendre une signature informatique identique.

Dans le but de personnaliser éventuellement le certificateur avec un système informatisé spécifique ou afin de

disposer du meilleur niveau de sécurité, un responsable qualifié, c'est-à-dire disposant :
- du code interne du module de mémoire,
- du code secret du module de mémoire,

peut modifier séparément ou globalement :
- le code secret du module de mémoire,
- le code standard de certification,
- la clef secrète de chiffrement,
- un, plusieurs ou la totalité des postes de la table de l'algorithme de certification enregistrés dans le module de mémoire.

L'utilisation du certificateur à mémorisation séquentielle afin d'apporter des modifications dans les informations enregistrées dans le module de mémoire, soit :
- le code secret,
- le code standard de certification,
- la clef secrète de chiffrement,
- l'une ou plusieurs des quatre zones réservées avec la carte à microprocesseur,

et d'authentifier l'identité d'une personne physique au cours d'une opération de connexion à un système informatisé, est caractérisé par un procédé, dont le raisonnement décomposé sur la figure 7, est décrit ci après :
- l'utilisateur procède à la mise sous tension manuelle (114) de l'appareil en positionnant l'interrupteur (16) : EN FONCTION,
- le message : IDENTIFIER s'affiche (115) sur l'écran (2),
- l'utilisateur appuie (116) sur la touche de fonction : IDENTIFIER (5),
- un message constitué de tirets est affiché (117) sur l'écran (2),
- l'utilisateur compose (118) le code d'identification du certificateur, par exemple : CNM12345 à l'aide du clavier alphanumérique (12),
- l'utilisateur appuie (119) sur la touche de fonction : ENTRER (10),
- un test du code composé (bloc 118) par l'utilisateur est effectué afin de déterminer (120) si ce code commence par les caractères alphabétiques : CNM. Dans la négative, le programme enregistré dans le module de mémoire du certifi-

cateur considère que la procédure en cours d'exécution correspond à une opération d'authentification d'identité et le contrôle du programme est transféré afin de poursuivre l'exécution à l'étape 164. Dans l'affirmative, un test de la valeur du code interne du module de mémoire est effectué afin de déterminer (121) si cette valeur est identique à celle composée (bloc 118) par l'utilisateur. Dans la négative le contrôle du programme est transféré afin de poursuivre l'exécution à l'étape 154, dans laquelle le message : ERREUR 1 s'affiche sur l'écran (2) puis le microprocesseur (3) procède (bloc 155) automatiquement à la mise hors tension de l'appareil. Dans le cas contraire, le message : AUTHENTIFIER s'affiche (122) sur l'écran (2),

- l'utilisateur appuie (123) sur la touche de fonction : AUTHENTIFIER (6),
- un message constitué de tirets est affiché (124) sur l'écran (2),
- l'utilisateur compose (125) le code secret du module de mémoire, par exemple : XYZXYZ12 à l'aide du clavier alphanumérique (12),
- l'utilisateur appuie (126) sur la touche de fonction : ENTRER (10),
- un test de la valeur du code conservé dans la zone : code secret du module de mémoire est effectué afin de déterminer (127) si cette valeur est égale au code secret composé (bloc 125) par l'utilisateur. Dans la négative, le message : ERREUR 2 s'affiche sur l'écran (2),
  - . l'utilisateur appuie (157) sur la touche de fonction : ENTRER (10),
  - . un test du nombre de fois ou le message : ERREUR 2 a été affiché est effectué (158). Si la valeur obtenue est inférieure ou égale à TROIS, le contrôle du programme est transféré afin de reprendre l'exécution à l'étape 115.
- Dans la négative, le programme enregistré dans le module de mémoire du certificateur procède (159) à la remise à zéro des postes de la table de certification enregistrée dans le module de mémoire.
- le programme enregistré dans le module de mémoire procède

(160) à la remise à la valeur initiale du code secret du module de mémoire. Cette valeur étant le code secret enregistré lors de la fabrication du module de mémoire, dans notre exemple : XYZXYZ12,

- le microprocesseur (3) procède automatiquement (161) à la mise hors tension du certificateur,
- si le test effectué (bloc 127) confirme l'égalité entre le code secret composé (bloc 125) et le code conservé dans la zone : code secret du module de mémoire, le message : INITIER s'affiche (128) sur l'écran (2),
- l'utilisateur appuie (129) sur la touche de fonction : INITIER (9),
- le message : CODE CMS s'affiche (130) sur l'écran (2),
- l'utilisateur compose (131) le nouveau code secret du module de mémoire, par exemple : ABCDEFGH à l'aide du clavier alphanumérique (12),
- l'utilisateur appuie (132) sur la touche de fonction : ENTRER (10),
- le message : AUTHENTIFIER s'affiche (133) sur l'écran (2),
- l'utilisateur appuie (134) sur la touche de fonction : AUTHENTIFIER (6),
- un message constitué de tirets est affiché (135) sur l'écran (2),
- l'utilisateur compose (136) une seconde fois le nouveau code secret du module de mémoire, par conséquent : ABCDEFGH à l'aide du clavier alphanumérique (12). Cette opération est destinée à s'assurer que le nouveau code secret est bien identique à celui composé en (bloc 131) de manière à éviter une erreur majeure, qui conduirait à une difficulté ultérieure de fonctionnement du certificateur,
- l'utilisateur appuie (137) sur la touche de fonction : ENTRER (10),
- un test de la valeur du code conservé dans la zone : code secret du module de mémoire est effectué afin de déterminer (138) si cette valeur est égale au code secret composé (bloc 131) par l'utilisateur. Dans la négative, le contrôle du programme est transféré afin de poursuivre l'exécution à l'étape 162, dans laquelle le message : ERREUR 3 s'affiche sur l'écran (2) puis le microprocesseur

(3) procède (bloc 163) automatiquement à la mise hors tension du certificateur,

- dans le cas contraire, le message : INITIER s'affiche (139) sur l'écran (2),
- l'utilisateur appuie (140) sur la touche de fonction : INITIER (9),
- le message : POSTE_ s'affiche (141) sur l'écran (2),
- l'utilisateur compose (142) le caractère alphanumérique ou hexadécimal qu'il souhaite voir afficher avant de le modifier, par exemple : A à l'aide du clavier alphanumérique (12),
- l'utilisateur appuie (143) sur la touche de fonction : ENTRER (10),
- les caractères numériques du poste de la table correspondant au caractère : A s'affichent (144) sur l'écran (2) permettant une vérification visuelle préalable à la modification, par exemple : 12180624,
- l'utilisateur compose (145) la nouvelle matrice correspondante au poste de la table de certification qu'il souhaite modifier, par exemple : 22151785 à l'aide du clavier alphanumérique (12),
- l'utilisateur appuie (146) sur la touche de fonction : ENTRER (10). Si l'utilisateur ne souhaite pas modifier le contenu d'un poste de la table de certification, il lui suffit de ne pas réaliser l'étape référencée (145),
- le message : POSTE_ s'affiche (147) sur l'écran (2),
- l'utilisateur procède (148) de manière identique pour effectuer la modification de l'ensemble des postes de la table de certification, en répétant les interventions décrites dans les étapes référencées 142 à 146. Pour introduire les caractères spéciaux, c'est-à-dire les caractères non représentés sur le clavier alphanumérique (12), l'utilisateur compose la combinaison de deux caractères : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F correspondant à la représentation hexadécimale de la valeur, par exemple : FF pour la valeur deux cent cinquante cinq,
- un test de la valeur introduite au cours de l'étape référencée 148 est effectué afin de déterminer (149) si le mot clef : FIN a été composé à la place d'un nouveau

poste de la table de certification. Dans la négative, le contrôle du programme est transféré pour exécution à l'étape référencée 148,

- sinon le message : CONFIRMER s'affiche sur l'écran (2),
- l'utilisateur compose (151) le mot clef : OUI ou le mot clef : NON à l'aide du clavier alphanumérique (12). La reconnaissance des caractères alphabétiques : OUI autorise le programme enregistré dans le module de mémoire à exécuter le traitement de mise à jour de la table de certification,
- l'utilisateur appuie (152) sur la touche de fonction : ENTRER (10). Toute chaîne de caractères différente de la chaîne de caractères : OUI , par exemple : ABC sera interprétée par le programme enregistré dans le module de mémoire comme étant une chaîne de caractères égale au mot clef : NON
- le microprocesseur (3) procède (153) automatiquement à la mise hors tension du certificateur,
- si le code composé (bloc 118) par l'utilisateur ne commence pas par les caractères : CNM le message : AUTHENTIFIER s'affiche (164) sur l'écran (2),
- l'utilisateur appuie (165) sur la touche de fonction : AUTHENTIFIER (6),
- un test est réalisé par le programme enregistré dans le module de mémoire interne afin de déterminer (166) s'il utilise le module de mémoire interne. Dans la négative, le contrôle du programme est transféré afin de poursuivre l'exécution à l'étape 178, dans laquelle le code interne du module de mémoire externe est affiché sur l'écran (2) et placé dans la zone de saisie, puis le contrôle du programme est transféré (179) afin de poursuivre l'exécution à l'étape 169,
- dans le cas contraire, un message constitué de tirets est affiché (167) sur l'écran (2),
- l'utilisateur compose (168) son code secret personnel, par exemple : CASIMODO à l'aide du clavier alphanumérique (12),
- l'utilisateur appuie (169) sur la touche de fonction : ENTRER (10),
- le message : CERTIFIER s'affiche (170) sur l'écran (2),

- l'utilisateur appuie (171) sur la touche de fonction : CERTIFIER (7),
- un message constitué de tirets est affiché (172) sur l'écran (2),
- l'utilisateur compose (173) le message que lui a délivré l'ordinateur et qui est affiché sur l'écran de visualisation de son terminal, soit dans l'exemple : ZDBXEC4F à l'aide du clavier alphanumérique (12),
- l'utilisateur appuie (174) sur la touche de fonction : ENTRER (10),
- le certificateur exploite (175) par l'exécution de l'algorithme de certification, les informations :
  . code d'identification de l'utilisateur,
  . code secret personnel de l'utilisateur,
  . message délivré par le système informatisé : ZDBXEC4F
  . table individuelle de certification,
- le résultat du traitement de l'algorithme de certification par le certificateur est affiché (176) sur l'écran (2) sous la forme d'une valeur de huit positions numériques, dans notre exemple : 28121456
- après l'exploitation par l'utilisateur de cette information dans le cadre de la procédure de connexion au système informatisé, l'utilisateur procède (177) manuellement à la mise hors tension du certificateur, à l'aide de l'interrupteur (16). En cas d'omission, cette mise hors tension sera réalisée automatiquement après un délai de trois minutes, par le microprocesseur (3) du certificateur.

En fonction de la table de certification enregistrée dans le module de mémoire du certificateur, le certificateur peut fonctionner avec des codes de certification de huit, douze ou seize chiffres. Dans ce cas, le certificateur adapte respectivement les instructions d'affichage à huit, douze ou seize caractères numériques et effectue les opérations en utilisant une arithmétique ayant pour base le plus grand nombre premier de deux, trois ou quatre chiffres décimaux en relation avec le contenu de la table de certification utilisée.

Le code de certification calculé remplace dans le module de mémoire le dernier code de certification généré, qui lui-même remplace l'avant dernier code de certification

généré.

L'utilisation du certificateur à mémorisation séquentielle dans le cadre d'une opération de certification d'informations sensibles afin d'authentifier un ordre donné, par la génération d'une signature informatique, est caractérisée par un procédé dont le raisonnement est décomposé sur la figure 8 et décrit ci après :

- mise sous tension manuelle (180) du certificateur en basculant l'interrupteur (16) sur la position : EN FONCTION,
- le message : IDENTIFIER s'affiche (181) sur l'écran (2),
- l'utilisateur appuie (182) sur la touche de fonction : IDENTIFIER (5),
- un message constitué de tirets est affiché (183) sur l'écran (2),
- l'utilisateur compose (184) le code d'identification, par exemple : DUPONT à l'aide du clavier alphanumérique (12),
- l'utilisateur appuie (185) sur la touche de fonction : ENTRER (10),
- le message : AUTHENTIFIER s'affiche (186) sur l'écran (2),
- l'utilisateur appuie (187) sur la touche de fonction : AUTHENTIFIER (6),
- un message constitué de tirets s'affiche (188) sur l'écran (2),
- l'utilisateur compose (189) son code secret personnel, par exemple : CASIMODO, puis appuie (190) sur la touche de fonction : ENTRER (10),
- le message : CERTIFIER s'affiche (191) sur l'écran (2),
- l'utilisateur appuie (192) sur la touche de fonction : CERTIFIER (7),
- un message constitué de tirets est affiché (193) sur l'écran (2),
- l'utilisateur compose (194) le message dont il souhaite la certification à l'aide du clavier alphanumérique (12), dans l'exemple : 123456789,
- l'utilisateur appuie (195) sur la touche de fonction : SIGNER (8),
- dans la mesure où le code d'identification et le code secret personnel de l'utilisateur correspondent à ceux conservés dans le module de mémoire du certificateur, le message à certifier est traité (196) par, soit :

. l'algorithme de certification,
. l'algorithme de chiffrement à clef publique,
. l'algorithme de chiffrement à clef secrète,
en fonction de l'option existante pour l'utilisateur dans le module de mémoire et dans le certificateur,

- le résultat du traitement par l'algorithme retenu est affiché (197) sur l'écran, éventuellement par l'intermédiaire de combinaisons de caractères hexadécimaux, si l'algorithme de chiffrement produit des valeurs non affichables par les caractères standard de l'écran (2),
- l'utilisateur procède à la mise hors tension (198) manuelle du certificateur à l'aide de l'interrupteur (16). En cas d'omission, cette mise hors tension sera réalisée automatiquement après un délai de trois minutes, par le microprocesseur (3) du certificateur. En fonction de l'option existante pour l'utilisateur, le code de certification calculé remplace dans le module de mémoire le dernier code de certification généré qui lui même remplace l'avant dernier code de certification généré, ou la dernière signature générée qui elle même remplace l'avant dernière signature générée.

L'utilisation du certificateur à mémorisation séquentielle dans le cadre d'une opération d'authentification d'identité par la génération d'une signature informatique est caractérisée par un procédé, dont le raisonnement est décomposé sur la figure 9 et est décrit ci après :

- mise sous tension manuelle (200) du certificateur en basculant l'interrupteur (16) sur la position : EN FONCTION,
- un message constitué de tirets s'affiche (201) sur l'écran (2),
- le responsable habilité compose (202) le code alphabétique caractérisant l'organisme concerné. Chaque tiret affiché sur l'écran (2), en partant de la gauche vers la droite, est effacé par l'introduction au clavier (12) d'un nouveau caractère. Cependant les caractères introduits ne sont pas affichés sur l'écran (2),
- le responsable habilité appuie (203) sur la touche de fonction : CERTIFIER,
- un message constitué de tirets s'affiche (204) sur l'écran (2),

- l'utilisateur compose (205) son code secret personnel, par exemple : PENELOPE à l'aide du clavier alphanumérique (12),
- chaque tiret affiché sur l'écran (2) en partant de la gauche vers la droite, est effacé par l'introduction au clavier d'un nouveau caractère. Cependant les caractères composés par l'utilisateur ne sont pas affichés,
- l'utilisateur appuie (206) sur la touche de fonction : SIGNER (8),
- le certificateur exploite (207) par l'exécution de l'algorithme retenu les informations :
  . code de l'organisme concerné, par exemple : ABCDEFGH
  . code secret personnel de l'utilisateur, par exemple : PENELOPE
  . postes de la table de certification,
- le résultat du traitement par l'algorithme retenu est affiché (208) sur l'écran (2),
- le responsable concerné compare (209) le résultat affiché sur l'écran (2) avec la valeur de référence, par exemple inscrite sur une carte de crédit, un chèque, etc ...
  . en cas d'égalité, la demande exprimée est acceptée,
  . dans le cas contraire, la demande exprimée est refusée,
- l'utilisateur procède à la mise hors tension manuelle (210) du certificateur à l'aide de l'interrupteur (16). En cas d'omission, cette mise hors tension sera réalisée automatiquement après un délai de trois minutes, par le microprocesseur (3) du certificateur. En fonction de l'option existante pour l'utilisateur, le code de certification calculé remplace dans le module de mémoire le dernier code de certification généré qui lui même remplace l'avant dernier code de certification généré, ou la dernière signature informatique qui elle même remplace l'avant dernière signature informatique générée.

Le certificateur à mémorisation séquentielle justifie pleinement sa dénomination lorsque l'utilisation de cet appareil, combiné avec le logiciel spécialisé d'un système informatisé est caractérisé par un procédé, dont le raisonnement est décomposé sur la figure 10 et est décrit ci après.

Lorsqu'un utilisateur exécute une procédure standard de

connexion à un système informatisé (211) il doit obligatoirement fournir un identifiant de connexion, par exemple : DUPONT et un code secret personnel. Si le code personnel de l'utilisateur correspond à celui conservé par le système informatisé, la connexion est autorisée.

Le procédé mis en oeuvre dans le certificateur à mémorisation séquentielle est le suivant :

- le certificateur est initié à une valeur déterminée, par exemple : 12345678
- l'utilisateur appuie sur la touche de fonction : CERTIFIER (7),
- l'algorithme de certification s'exécute sur la valeur : 12345678. La certification associe à chaque chiffre une matrice de rang deux, c'est-à-dire composée d'un tableau carré de quatre nombres. Le programme enregistré dans le module de mémoire effectue en chaîne les produits des matrices de tous les chiffres impliqués. Afin d'éliminer les risques de dépassement, les calculs sont opérés en utilisant une arithmétique ayant pour base le plus grand nombre premier de deux, trois ou quatre chiffres en relation avec le contenu de la table de certification utilisée. La table de certification est personnalisée à chaque utilisateur en fonction de son identifiant. Le résultat de l'algorithme est :
  . affiché sur l'écran (2) du certificateur,
  . conservé dans le module de mémoire où il remplace le dernier code de certification qui lui même remplace l'avant dernier code de certification,
- l'utilisateur communique ce résultat au système informatisé (211) par exemple : 96708069
- le système informatisé qui a été initié pour l'utilisateur : DUPONT à la valeur : 12345678 personnalise la table standard de certification en fonction de l'identifiant : DUPONT puis exécute le même algorithme. Il compare le résultat et en cas d'égalité :
  . autorise la connexion de l'usager,
  . remplace la valeur : 12345678 par le résultat de l'algorithme : 96708069 dans la zone : code secret de l'utilisateur : DUPONT, sinon il refuse la connexion et conserve la valeur : 12345678 en l'état,

- lors de la connexion suivant (212), le même procédé est répété et le résultat obtenu est à présent : 65602613
- et ainsi de suite (213) dont le résultat est : 60234462

Ce procédé d'utilisation apporte les plus grandes conditions de sécurité. Le déroulé opératoire est pratiquement identique à celui exposé sur la figure 3 :

- mise sous tension manuelle (66) du certificateur en basculant l'interrupteur (16) sur la position : EN FONCTION,
- le message : IDENTIFIER s'affiche (67) sur l'écran (2),
- l'utilisateur appuie (68) sur la touche de fonction : IDENTIFIER (5),
- un message constitué de tirets est affiché (69) sur l'écran (2),
- l'utilisateur compose (70) son code d'identification, par exemple : DUPONT à l'aide du clavier alphanumérique (12),
- l'utilisateur appuie (71) sur la touche de fonction : ENTRER (10),
- le message : AUTHENTIFIER s'affiche (72) sur l'écran (2),
- l'utilisateur appuie (73) sur la touche de fonction : AUTHENTIFIER (6),
- un message constitué de tirets est affiché (74) sur l'écran (2),
- l'utilisateur compose (75) son code secret personnel, par exemple : CASIMODO, puis appuie (76) sur la touche de fonction : ENTRER (10),
- le message : CERTIFIER s'affiche (77) sur l'écran (2),
- l'utilisateur appuie (78) deux fois de suite sur la touche de fonction : CERTIFIER (7),
- Le certificateur exploite (82) par l'exécution de l'algorithme de certification les informations :
  . code d'identification : DUPONT
  . dernier code de certification conservé dans la zone appropriée du module de mémoire,
- le résultat du traitement de l'algorithme de certification par le certificateur est :
  . affiché (83) sur l'écran (2),
  . conservé dans la zone : dernier code de certification généré, qui elle même remplace l'avant dernier code de

certification généré, du module de mémoire du certificateur,

- l'utilisateur compose sur le clavier de son terminal connecté au système informatisé, le code de certification élaboré par le certificateur à mémorisation séquentielle, dans notre exemple : 28121456 et son code d'identification DUPONT
- le terminal le transmet au système informatisé (211). Le logiciel spécialisé du système informatisé exécute à son tour l'algorithme de certification puis effectue la comparaison entre le code transmis par l'utilisateur et le résultat obtenu. Si les deux codes sont identiques, l'ordinateur authentifie l'utilisateur. Dans le cas contraire, l'ordinateur refuse l'accès de l'utilisateur et prend les dispositions qui s'imposent afin de procéder à son rejet du système informatisé.
- pour terminer, l'utilisateur procède à la mise hors tension manuelle (84) du certificateur à l'aide de l'interrupteur (16). En cas d'omission, cette mise hors tension sera réalisée automatiquement après un délai de trois minutes par le microprocesseur (3) du certificateur.

Le certificateur à mémorisation séquentielle est autonome et portatif.

Cependant les trois composants principaux :

- le microprocesseur (3),
- le module de mémoire interne (4),
- le mécanisme de lecture (13) de la carte à microprocesseur,

peuvent être incorporés dans un autre appareil, par exemple le clavier d'un terminal d'ordinateur ou dans le clavier d'un MINITEL. Dans ce cas, l'écran du terminal ou du MINITEL remplace l'écran (2) du certificateur et, le clavier du terminal ou du MINITEL remplace le clavier alphanumérique (12) du certificateur.

Cependant les concepts et procédé pour fonctionner demeurent identiques à ceux mis en oeuvre pour un certificateur à mémorisation séquentielle autonome.

REVENDICATIONS

1) Certificateur à mémorisation séquentielle, caractérisé en ce qu'il comporte un carter (1), un écran d'affichage (2) positionné en haut de la face supérieure du carter permettant la représentation de caractères alphanumériques et spéciaux, un microprocesseur (3), un module de mémoire enfichable de 16 K/octets (4) dans lequel sont enregistrés les informations fixes et variables modifiables par l'utilisateur et le programme informatique chargé d'orienter les instructions que doit exécuter le microprocesseur, une touche de fonction IDENTIFIER (5), une touche de fonction AUTHENTIFIER (6), une touche de fonction CERTIFIER (7), une touche de fonction SIGNER (8), une touche de fonction INITIER (9), une touche de fonction ENTRER (10), une touche de fonction EFFACER (11), vingt six touches permettant de composer les vingt six caractères de l'alphabet latin, dix touches permettant de composer les dix chiffres arabes, deux touches de défilement permettant de déplacer le curseur d'affichage vers la droite ou vers la gauche, ou bien d'afficher le code de certification précédent ou en cours (12), une fente (13) permettant d'introduire une carte à microprocesseur (14) dans un mécanisme spécialisé de lecture, un interrupteur (16) permettant d'assurer la mise sous tension et hors tension manuelle du certificateur, un lecteur de carte à microprocesseur.

2) Certificateur à mémorisation séquentielle selon la revendication 1, caractérisé en ce que la touche de fonction référencée : IDENTIFIER (5) permet de diriger le microprocesseur vers la séquence d'instructions enregistrée dans le module de mémoire chargée de gérer l'ensemble fonctionnel destiné à identifier un utilisateur.

3) Certificateur à mémorisation séquentielle selon la revendication 1, caractérisé en ce que la touche de fonction référencée : AUTHENTIFIER (6) permet de diriger le microprocesseur vers la séquence d'instructions enregistrée dans le module de mémoire chargée de gérer l'ensemble fonctionnel destiné à authentifier un utilisateur.

4) Certificateur à mémorisation séquentielle selon la revendication 1, caractérisé en ce que la touche de fonction référencée : CERTIFIER (7) permet de diriger le microprocesseur vers la séquence d'instructions enregistrée dans le module de mémoire chargée de gérer l'ensemble fonctionnel

destiné à certifier les informations collectées auprès de l'utilisateur, en exécutant un algorithme de certification ou un algorithme de chiffrement à clef publique ou à clef secrète, puis à :

- communiquer le résultat à l'usager par l'intermédiaire de l'écran d'affichage,
- enregistrer le résultat dans les deux zones spécialisées du module de mémoire, afin de conserver les deux derniers codes de certification générés par le certificateur.

5) Certificateur à mémorisation séquentielle selon la revendication 1, caractérisé en ce que la touche de fonction référencée : SIGNER (8) permet de diriger le microprocesseur vers la séquence d'instructions enregistrée dans le module de mémoire chargée de gérer l'ensemble fonctionnel destiné à élaborer la signature informatique à partir des informations collectées auprès d'un responsable concerné et/ou d'un utilisateur, en exécutant un algorithme de certification ou un algorithme de chiffrement à clef publique ou à clef secrète, puis à :

- communiquer le résultat à l'usager par l'intermédiaire de l'écran d'affichage,
- enregistrer le résultat dans les deux zones spécialisées du module de mémoire afin de conserver les deux dernières signatures informatiques générées par le certificateur.

6) Certificateur à mémorisation séquentielle selon la revendication 1, caractérisé en ce que la touche de fonction référencée : INITIER (9) permet de diriger le microprocesseur vers la séquence d'instructions chargée de gérer l'ensemble fonctionnel destiné à permettre la modification dans le module de mémoire :

- du code secret de ce module,
- du code standard de certification,
- de la clef secrète de chiffrement de ce module,
- de l'une quelconque des quatre zones réservées au dialogue entre la carte à microprocesseur et le certificateur.
- de l'une quelconque des trente et une entrées de la table des utilisateurs dans laquelle sont enregistrées pour chacun d'entre eux :
  . son identité,
  . son code secret personnel et/ou de sa carte à micropro-

cesseur,
. sa clef publique de chiffrement,
. sa clef secrète de chiffrement,
. le dernier code de certification généré,
. l'avant dernier code de certification généré,
. la dernière signature informatique générée,
. l'avant dernière signature informatique générée,
- de l'un quelconque des deux cent cinquante six postes de la table de certification utilisée par l'algorithme de certification.

7) Certificateur à mémorisation séquentielle selon l'une des revendications 1 à 6 caractérisé en ce que les touches de fonction référencées : ENTRER (10) et EFFACER (11) permettent de diriger le microprocesseur vers la séquence de programme chargée d'exécuter les instructions prévues pour les ensembles fonctionnels : Identifier, Authentifier, Certifier, Initier, Signer, selon la touche de fonction qui a été appuyée au préalable par l'utilisateur d'une part, et caractérisé en ce que l'authentification d'identité se base sur la communication à l'usager d'une signature informatique,inscrite sur l'écran d'affichage du certificateur d'autre part.

8) Certificateur à mémorisation séquentielle, selon les revendications 1 et 7 caractérisé en ce que la signature informatique générée par le certificateur dépend d'un procédé informatisé de traitement algorithmique exécuté par le microprocesseur, à partir d'un programme résidant dans le module de mémoire, utilisant les informations communiquées par l'utilisateur au moyen :

- du clavier (12), à savoir :
  . son code d'identification,
  . son code secret personnel ou le code secret enregistré dans la mémoire d'une carte à microprocesseur après validation par l'utilisateur,
  . le code aléatoire, délivré généralement par le logiciel spécialisé d'un système informatisé et/ou le dernier code de certification généré par le certificateur et qui est conservé dans la zone spécialisée du module de mémoire.
- du lecteur de carte à microprocesseur après validation par l'utilisateur.

9) Certificateur à mémorisation séquentielle selon les revendications 1, 7 et 8, caractérisé en ce que les informations introduites sont traitées par un procédé algorithmique qui en fonction du choix du mode de fonctionnement initié pour chaque usager peut être :

- la certification qui associe, par l'intermédiaire de la table de certification éventuellement personnalisée par l'identité de l'utilisateur, chaque caractère en partant de la gauche vers la droite, à une matrice de rang deux, c'est-à-dire d'un tableau carré de quatre nombres, puis effectue en chaîne les produits de chaque matrice obtenue, en utilisant une arithmétique ayant pour base le plus grand nombre premier de deux, trois ou quatre chiffres en fonction du contenu de la table de certification utilisée,
- le chiffrement par l'intermédiaire d'une clef publique ou d'une clef secrète spécifique à chaque utilisateur, produisant un code chiffré affichable sur l'écran du certificateur et compréhensible par l'usager.

10) Certificateur à mémorisation séquentielle selon les revendications 1 à 9, caractérisé par un procédé d'authentification reposant sur la comparaison manuelle ou automatique de signatures informatiques résultant d'un traitement algorithmique exécuté à partir d'informations identiques dans :

- un certificateur à mémorisation séquentielle,
- un système informatisé,
- un autre certificateur à mémorisation séquentielle.

Planche 1/14

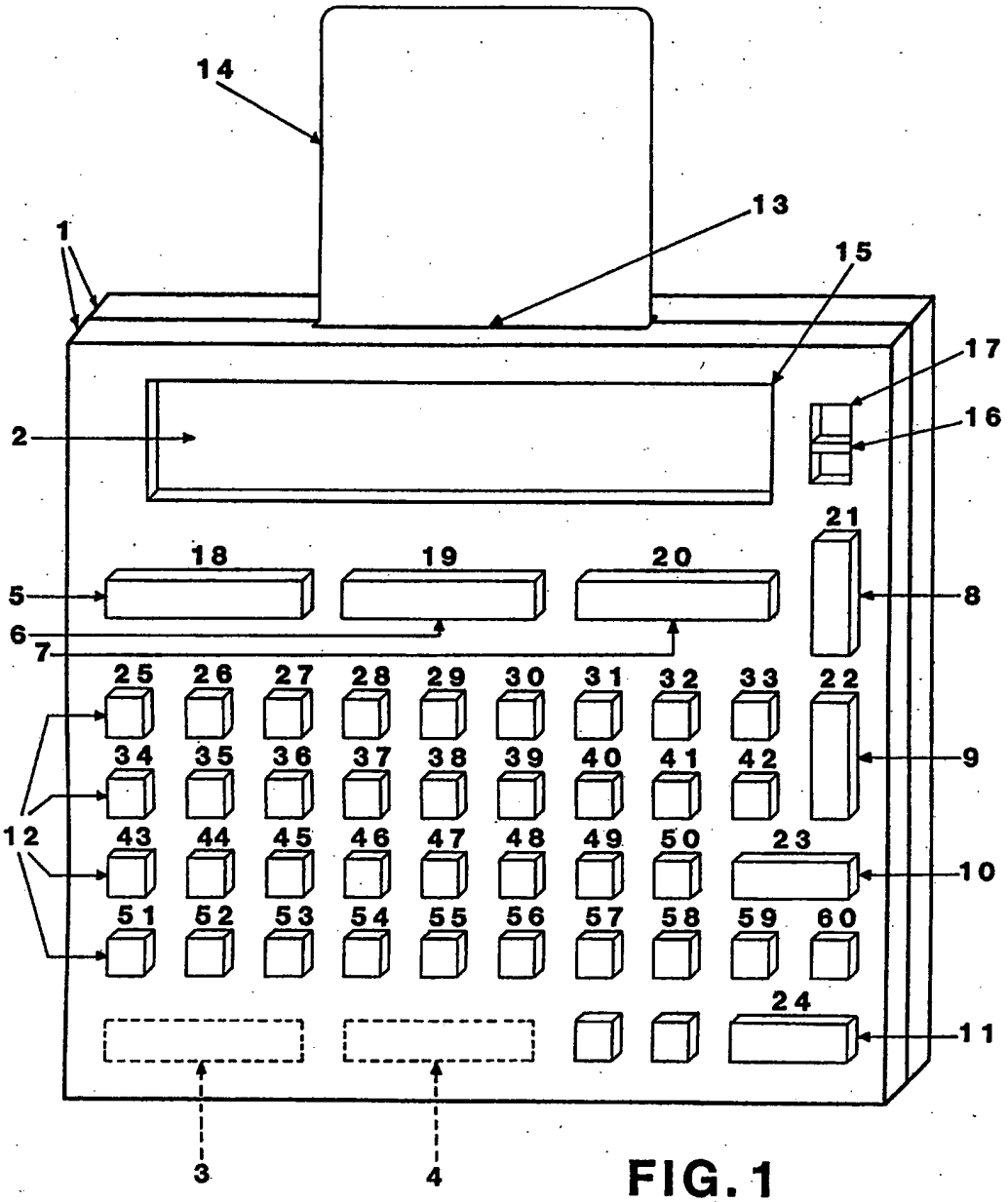
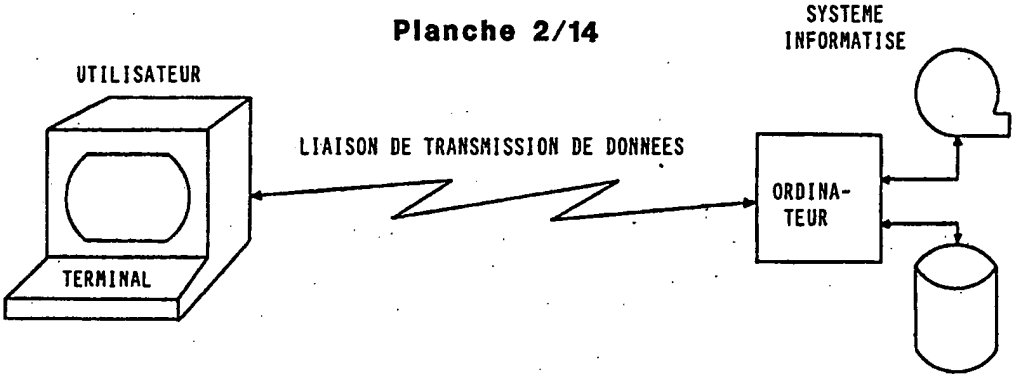


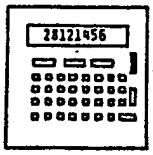
FIG. 1

Planche 2/14



DUPONT — DUPONT (61) → DUPONT

ZDBXEC4F — ZDBXEC4F (62) ← ZDBXEC4F

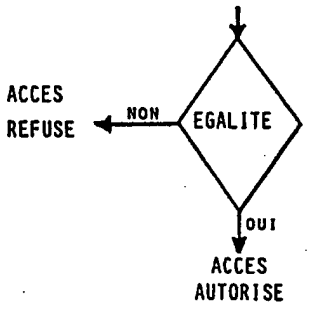


CODE D'IDENTIFICATION : DUPONT
CODE SECRET PERSONNEL : CASIMODO
CODE ALEATOIRE : ZDBXEC4F (63)
TABLE DE CERTIFICATION INDIVIDUELLE
= 28121456

28121456 — 28121456 (64) → 28121456

DUPONT
CASIMODO
ZDBXEC4F
(65) TABLE INDIVIDUELLE
= 28121456

FIG.2



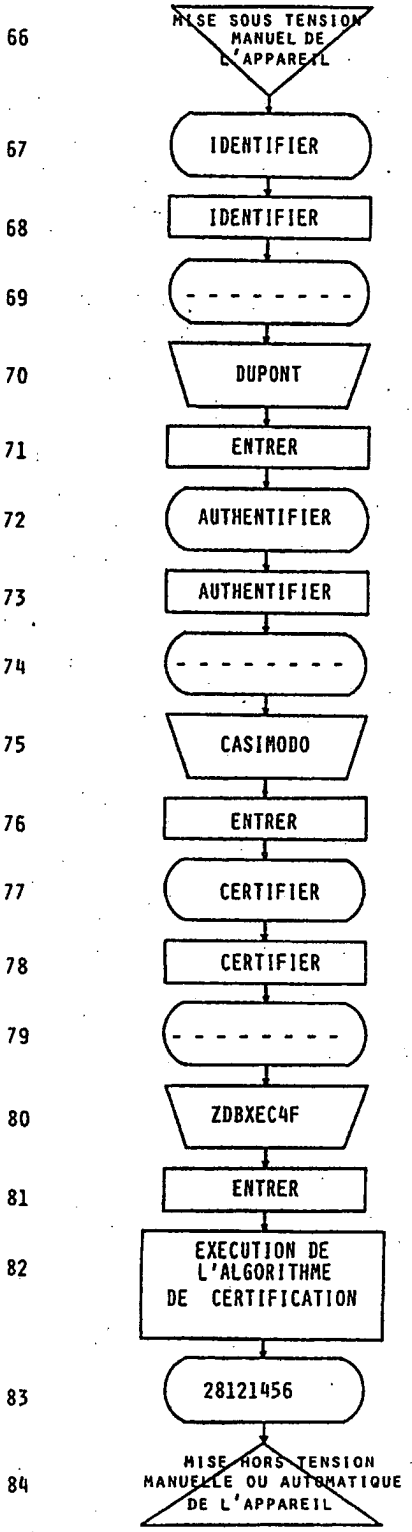

66
MISE SOUS TENSION MANUEL DE L'APPAREIL
67
IDENTIFIER
68
IDENTIFIER
69
- - - - - - - -
70
DUPONT
71
ENTRER
72
AUTHENTIFIER
73
AUTHENTIFIER
74
- - - - - - - -
75
CASIMODO
76
ENTRER
77
CERTIFIER
78
CERTIFIER
79
- - - - - - - -
80
ZDBXEC4F
81
ENTRER
82
EXECUTION DE L'ALGORITHME DE CERTIFICATION
83
28121456
84
MISE HORS TENSION MANUELLE OU AUTOMATIQUE DE L'APPAREIL

FIG.3

Planche 4/14

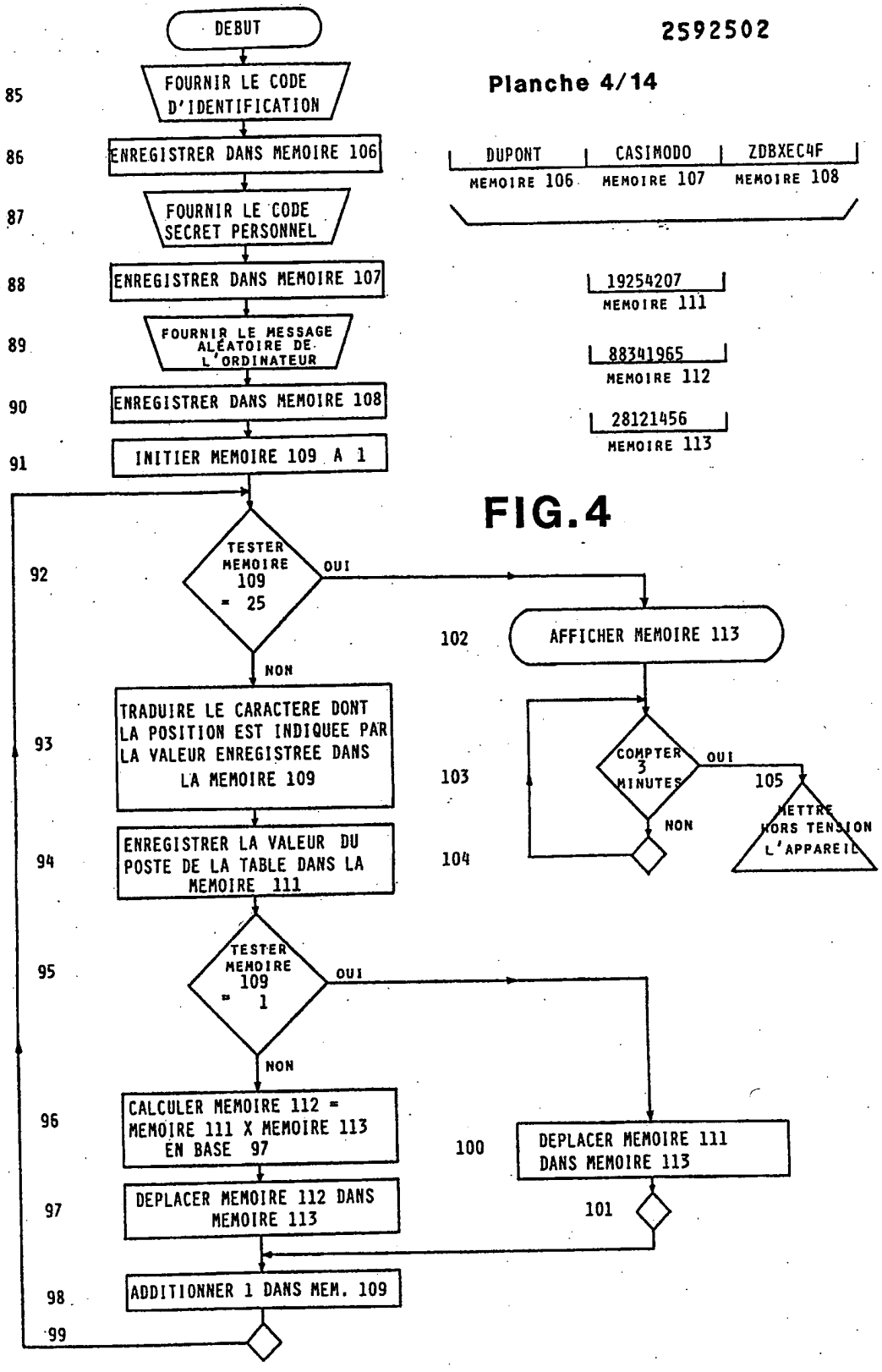


FIG.4

Planche 5/14

0	18	83	8	20
1	43	31	36	37
2	75	86	41	12
3	72	34	2	13
4	84	10	13	12
5	36	12	42	60
6	23	42	72	56
7	20	87	45	80
8	37	59	66	6
9	11	47	87	38
A	11	95	33	22
B	10	4	26	61
C	81	82	1	48
D	36	53	41	53
E	79	35	56	35
F	86	38	24	46
G	32	31	71	73
H	62	7	82	49
I	62	54	25	85
J	11	22	30	2
K	73	28	91	37
L	36	26	59	90
M	61	37	44	34
N	8	1	75	41
O	12	63	29	36
P	32	6	25	25
Q	93	73	26	17
R	91	53	20	5
S	25	11	78	49
T	15	73	26	9
U	79	56	57	66
V	96	56	77	67
W	41	93	73	73
X	68	72	79	35
Y	49	50	2	89
Z	54	81	22	85
-	24	96	63	38 (TIRET)

FIG.5

Planche 6/14

0	539	620	929	425
1	493	936	310	142
2	350	959	211	476
3	393	409	355	286
4	067	397	903	455
5	267	124	880	771
6	772	418	084	176
7	112	075	820	274
8	857	630	703	254
9	103	283	953	984
A	856	367	897	960
B	458	018	353	036
C	445	402	568	912
D	893	026	469	917
E	188	847	285	049
F	036	473	625	210
G	352	294	906	423
H	018	208	824	504
I	530	569	108	957
J	177	808	873	155
K	273	456	730	800
L	065	494	222	967
M	785	009	238	888
N	445	228	144	782
O	077	010	783	285
P	705	275	028	984
Q	157	754	867	037
R	068	378	585	541
S	195	955	358	854
T	907	818	060	955
U	095	177	094	512
V	975	461	931	785
W	313	748	281	197
X	420	630	725	423
Y	226	832	833	447
Z	238	927	937	089
-	969	735	803	172

FIG.6

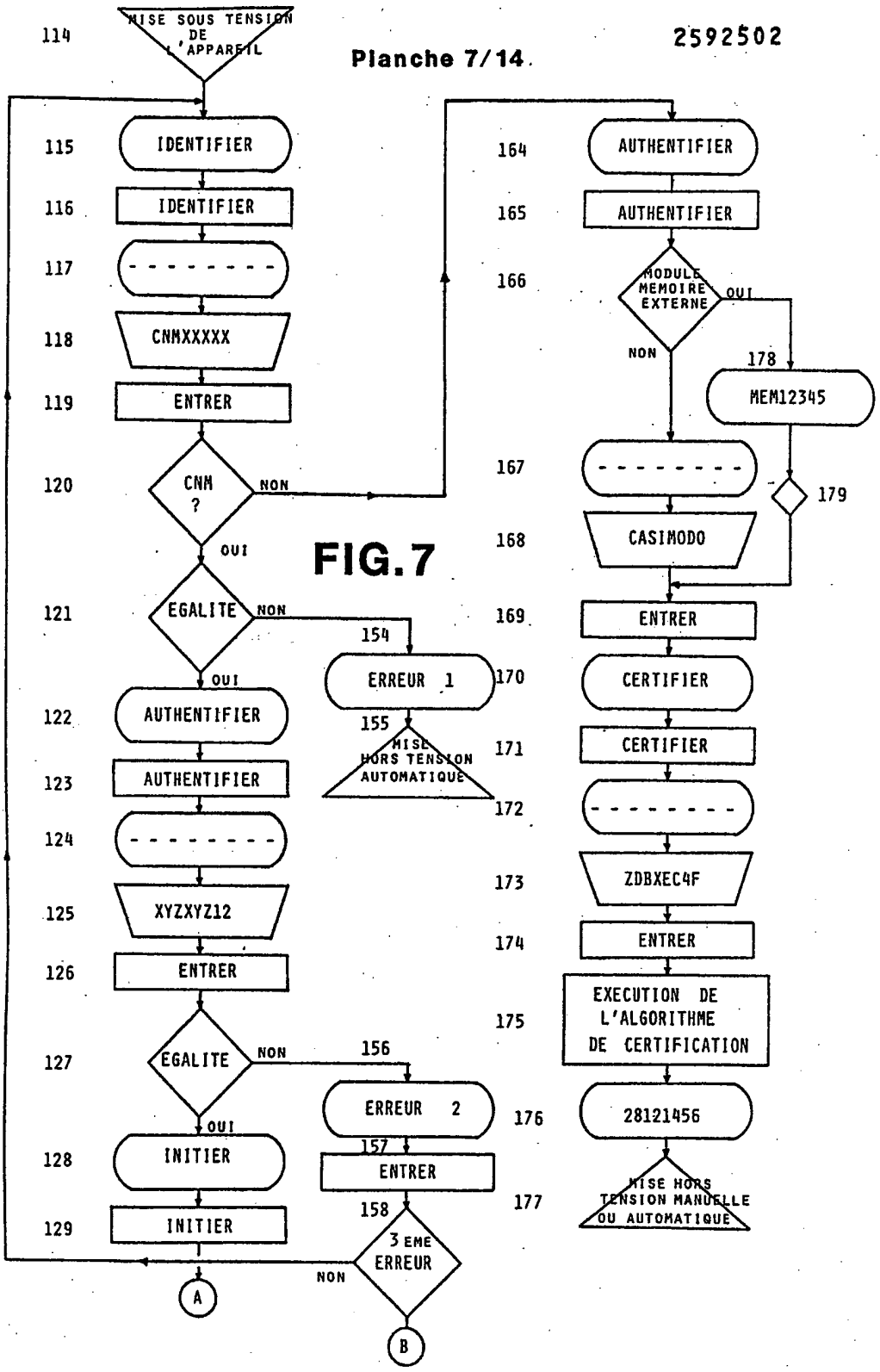

114
MISE SOUS TENSION DE L'APPAREIL
115
IDENTIFIER
116
IDENTIFIER
117
- - - - - - - -
118
CNMXXXXX
119
ENTRER
120
CNM ?
NON
OUI
121
EGALITE
NON
OUI
122
AUTHENTIFIER
123
AUTHENTIFIER
124
- - - - - - - -
125
XYZXYZ12
126
ENTRER
127
EGALITE
NON
OUI
128
INITIER
129
INITIER
154
ERREUR 1
155
MISE HORS TENSION AUTOMATIQUE
156
ERREUR 2
157
ENTRER
158
3 EME ERREUR
NON
A
B
164
AUTHENTIFIER
165
AUTHENTIFIER
166
MODULE MEMOIRE EXTERNE
OUI
NON
178
MEM12345
167
- - - - - - - -
179
168
CASIMODO
169
ENTRER
170
CERTIFIER
171
CERTIFIER
172
- - - - - - - -
173
ZDBXEC4F
174
ENTRER
175
EXECUTION DE L'ALGORITHME DE CERTIFICATION
176
28121456
177
MISE HORS TENSION MANUELLE OU AUTOMATIQUE

FIG.7

Planche 8/14

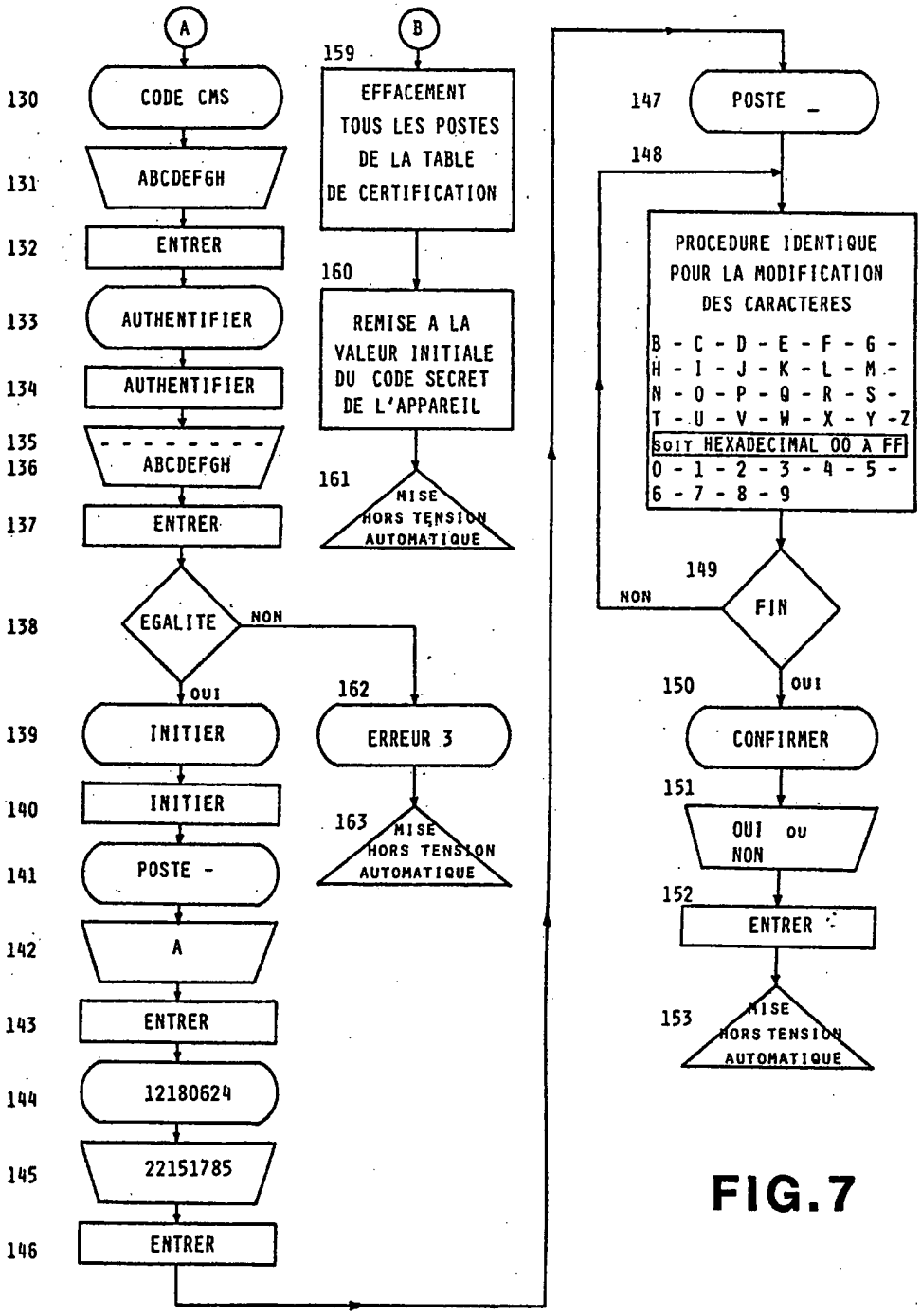


FIG.7

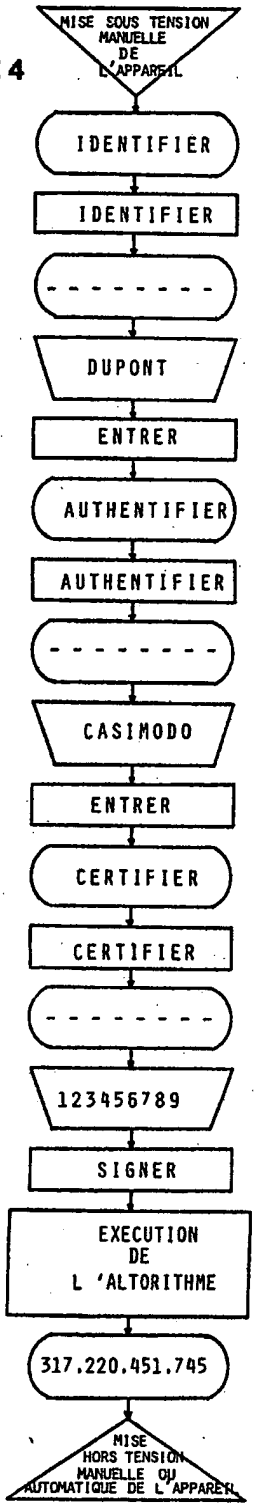

MISE SOUS TENSION MANUELLE DE L'APPAREIL
IDENTIFIER
IDENTIFIER
- - - - - - - -
DUPONT
ENTRER
AUTHENTIFIER
AUTHENTIFIER
- - - - - - - -
CASIMODO
ENTRER
CERTIFIER
CERTIFIER
- - - - - - - -
123456789
SIGNER
EXECUTION DE L 'ALTORITHME
317.220.451.745
MISE HORS TENSION MANUELLE OU AUTOMATIQUE DE L'APPAREIL
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198

FIG.8

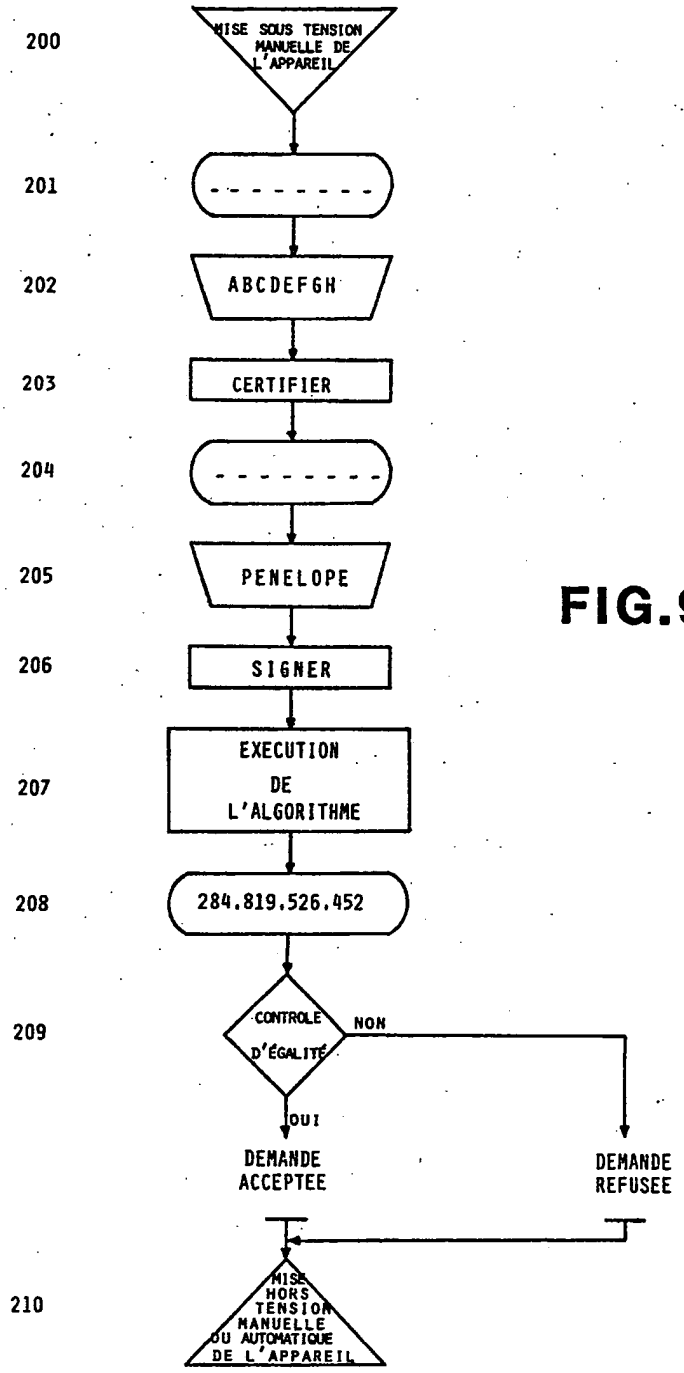

200
MISE SOUS TENSION MANUELLE DE L'APPAREIL
201
- - - - - - - -
202
ABCDEFGH
203
CERTIFIER
204
- - - - - - - -
205
PENELOPE
206
SIGNER
207
EXECUTION DE L'ALGORITHME
208
284.819.526.452
209
CONTROLE D'ÉGALITÉ
NON
OUI
DEMANDE ACCEPTEE
DEMANDE REFUSEE
210
MISE HORS TENSION MANUELLE OU AUTOMATIQUE DE L'APPAREIL

FIG.9

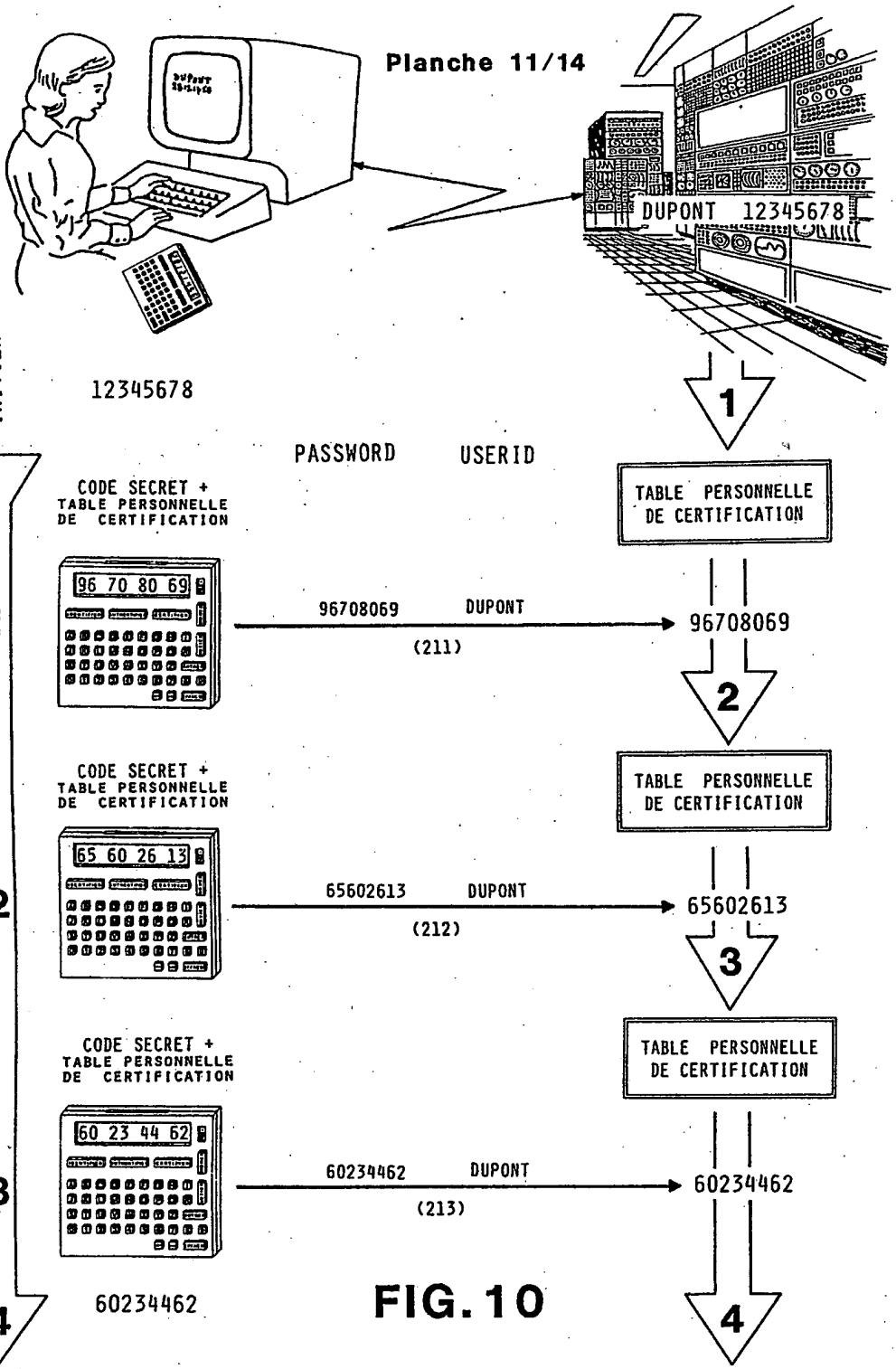

DUPONT 12345678
INITIER
12345678
PASSWORD
USERID
1
TABLE PERSONNELLE DE CERTIFICATION
CODE SECRET + TABLE PERSONNELLE DE CERTIFICATION
96 70 80 69
96708069 DUPONT
(211)
96708069
2
TABLE PERSONNELLE DE CERTIFICATION
CODE SECRET + TABLE PERSONNELLE DE CERTIFICATION
65 60 26 13
65602613 DUPONT
(212)
65602613
3
TABLE PERSONNELLE DE CERTIFICATION
CODE SECRET + TABLE PERSONNELLE DE CERTIFICATION
60 23 44 62
60234462 DUPONT
(213)
60234462
4
60234462

FIG. 10

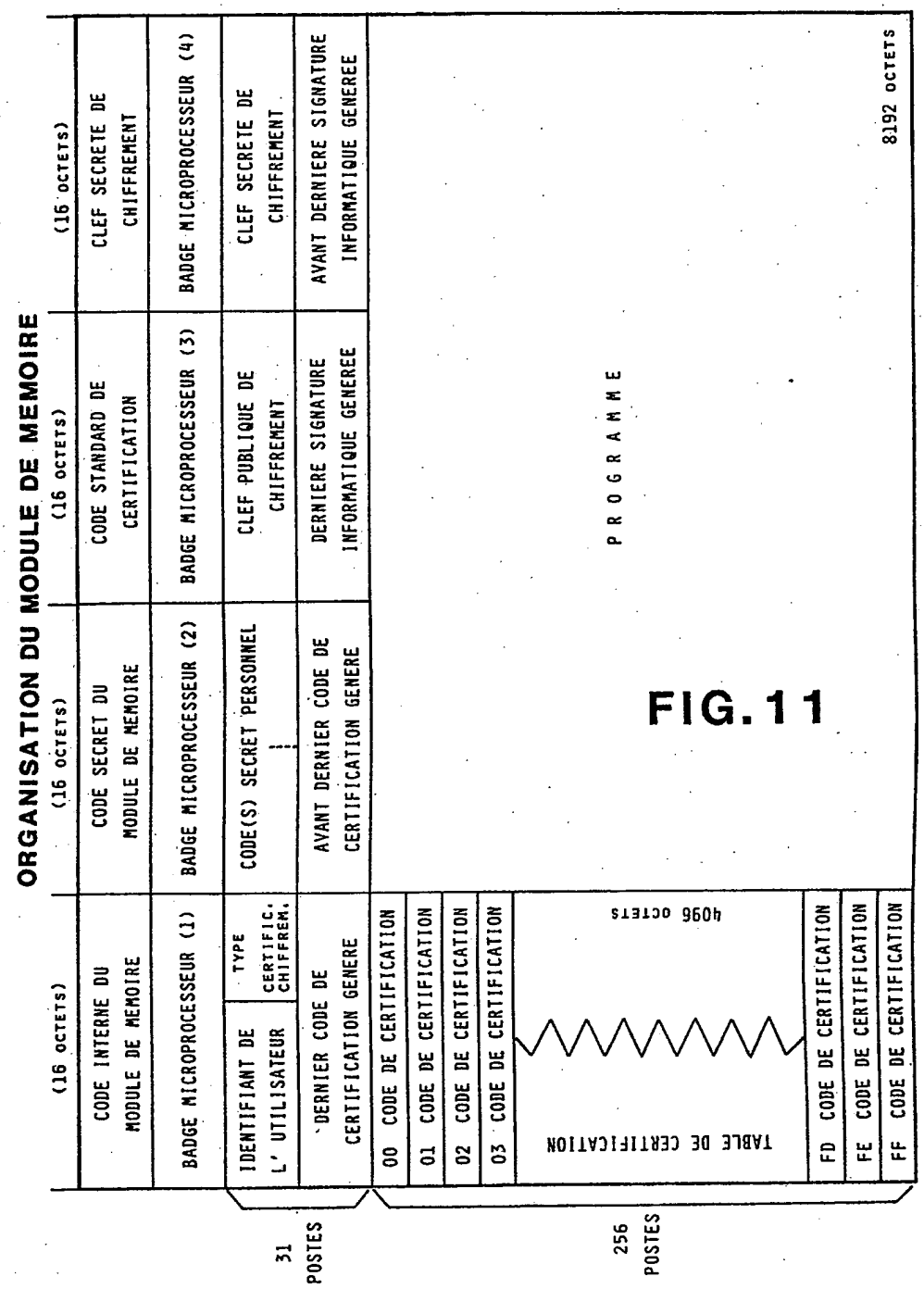

ORGANISATION DU MODULE DE MEMOIRE
(16 OCTETS)
(16 OCTETS)
(16 OCTETS)
CODE INTERNE DU MODULE DE MEMOIRE
CODE SECRET DU MODULE DE MEMOIRE
CODE STANDARD DE CERTIFICATION
CLEF SECRETE DE CHIFFREMENT
BADGE MICROPROCESSEUR (1)
BADGE MICROPROCESSEUR (2)
BADGE MICROPROCESSEUR (3)
BADGE MICROPROCESSEUR (4)
IDENTIFIANT DE L' UTILISATEUR
TYPE CERTIFIC. CHIFFREM.
CODE(S) SECRET PERSONNEL
CLEF PUBLIQUE DE CHIFFREMENT
CLEF SECRETE DE CHIFFREMENT
DERNIER CODE DE CERTIFICATION GENERE
AVANT DERNIER CODE DE CERTIFICATION GENERE
DERNIERE SIGNATURE INFORMATIQUE GENEREE
AVANT DERNIERE SIGNATURE INFORMATIQUE GENEREE
31 POSTES
00 CODE DE CERTIFICATION
01 CODE DE CERTIFICATION
02 CODE DE CERTIFICATION
03 CODE DE CERTIFICATION
TABLE DE CERTIFICATION
4096 OCTETS
FD CODE DE CERTIFICATION
FE CODE DE CERTIFICATION
FF CODE DE CERTIFICATION
256 POSTES
PROGRAMME
8192 OCTETS
16384 OCTETS

FIG.11

Planche 13/14

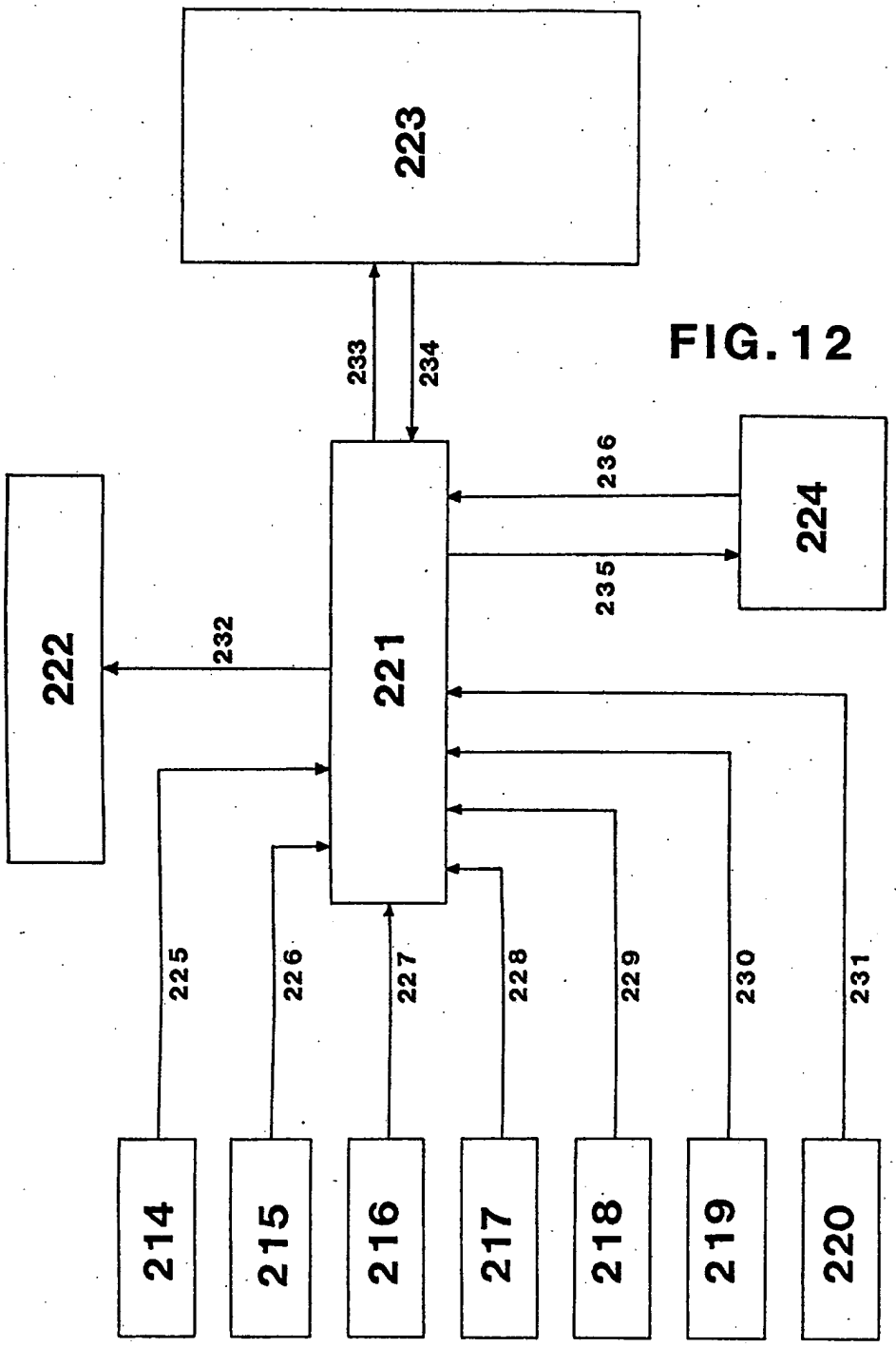


FIG. 12

Planche 14/14

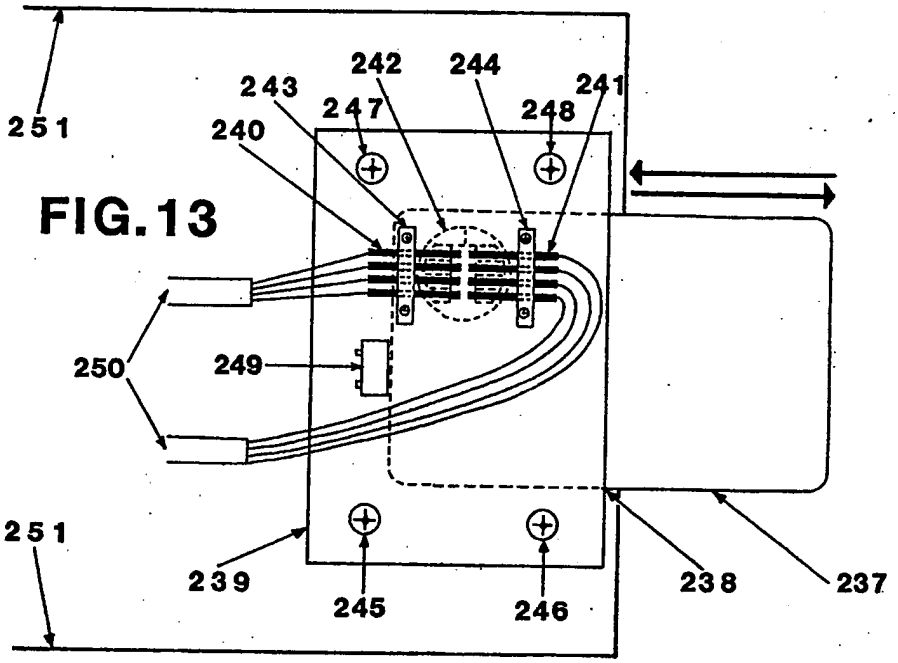


FIG. 13

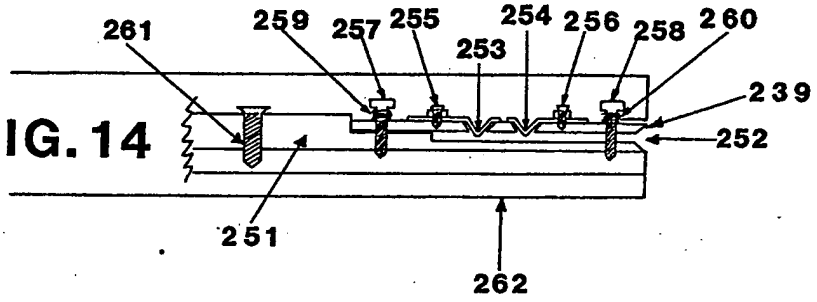


FIG. 14

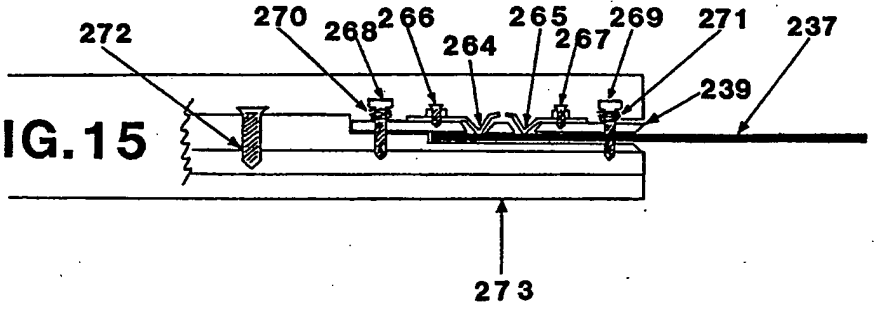


FIG. 15